

Enclosure to NCIA/COO/2025/01415



This page is left blank intentionally

Table of Contents

NCI AGENCY	3
2026 Service Rates v10.2	3
2026 Service Rates for NATO HQ* only	42
INTRODUCTION TO THE NCI AGENCY COSTED CUSTOMER SERVICES CATALOGUE	54
RETIRED SERVICES/FLAVOURS CURRENTLY SUPPORTED	64
REFERENCES.....	65
THE CATALOGUE	65
SERVICE.....	66
SERVICE PORTFOLIO GROUPINGS	67
SERVICE DELIVERY LIFECYCLE STAGES	68
PRODUCT	69
VALUE ADDED SERVICE.....	70
SERVICE & PRODUCT ATTRIBUTES	70
NCI AGENCY EDUCATION AND TRAINING SERVICES	73
NCI AGENCY SERVICES NOT COVERED BY THE COSTED CUSTOMER SERVICES CATALOGUE	73
COSTED CUSTOMER SERVICES CATALOGUE - DEFINITIONS	76
NATO DIGITAL WORKPLACE SERVICES	78
<i>NDW001 NATO Digital Workplace Service (Low Side)</i>	79
<i>NDW002 NATO Digital Workplace Service (High Side)</i>	83
<i>NDW003 Personal Workspace – Managed Device Service</i>	87
<i>NDW005 Digital Events Service</i>	93
<i>NDW006 Information and Knowledge Management Applications</i>	98
<i>NDW007 NATO AI Chatbot</i>	103
WORKPLACE SERVICES	105
<i>WPS001 Managed Device Services</i>	106
<i>WPS002 Enterprise Identity Access Management Service</i>	107
<i>WPS003 Enterprise User License Service</i>	111
<i>WPS006 REACH Mobile Workplace Service</i>	113
<i>WPS007 Print/ Scan/ Copy Service</i>	115
<i>WPS009 Unclassified Voice Collaboration Service</i>	120
<i>WPS010 Video (VTC) Collaboration Service</i>	123
<i>WPS011 IP Television (IPTV) Service</i>	126
<i>WPS012 Workstream Collaboration Service</i>	128
<i>WPS014 Secure Voice Service</i>	131

<i>WPS015 Voice Loop Service</i>	134
<i>WPS016 Enterprise Managed Mobility Service</i>	135
INFRASTRUCTURE SERVICES	140
<i>INF001 Local Area Network (LAN) Service</i>	141
<i>INF002 NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service</i>	143
<i>INF003 Enterprise Internet Access Service</i>	146
<i>INF004 Infrastructure Virtualization Service</i>	148
<i>INF005 Infrastructure Integration Service</i>	151
<i>INF006 NATO Enterprise Directory Service (NEDS)</i>	153
<i>INF007 Infrastructure Storage Service</i>	156
<i>INF012 SATCOM Service</i>	159
<i>INF013 NATO CIS (VLF) Mission Support for Submarine Operations Very Low Frequency (VLF) Broadcast Service</i>	163
<i>INF014 Transmission Service</i>	165
<i>INF015 Broadcast, Maritime Rear Link and Ship-Shore (BRASS) STIV RMD Service</i>	167
<i>INF016 Infrastructure Backup Service</i>	170
<i>INF020 DCIS – Deployable CIS Equipment Pool (DCEP) Service</i>	174
<i>INF023 Contingency Network Service</i>	179
<i>INF028 ACCS Sensor Integration Module (ASIM) Service</i>	180
<i>INF029 NATO High Frequency (HF) Support Service</i>	185
<i>INF034 Recognized Air Picture (RAP) Dissemination Service</i>	187
<i>INF035 DCIS – Deployable CIS Nodes Service for Land Based Users (LBU)</i>	189
<i>INF036 DCIS – Deployable SATCOM Service</i>	197
<i>INF037 DCIS – Deployable Radio Transmission Service</i>	203
<i>INF038 DCIS – Deployable Nodes Anchor Service</i>	206
<i>INF040 Ultra High Frequency (UHF) Tactical Satellite (TACSAT) Radio Services</i>	211
<i>INF041 CRC System Interface (CSI) Local Support Service</i>	213
<i>INF042 ADatP-3 Gateway Service</i>	214
<i>INF043 NATO Partner Network Service</i>	216
<i>INF049 Air Traffic Management (ATM) Gateway (GW) Service</i>	218
<i>INF053 Internet Website Publishing and Protection Service</i>	220
<i>INF055 DCIS - Mission Adaptable Reference System (MARS) Service</i>	222
<i>INF056 DCIS Nodes – Deployable CIS Nodes for Maritime Based Users (MBU)</i>	225
<i>INF060 GP DCIS – General Purpose Deployable CIS</i>	231
<i>INF062 NS MOBILE IT CAPABILITY – NSMOB – HERMES PACKAGE (HERMES)</i>	233
PLATFORM SERVICES	237
<i>PLT001 Information Sharing and Collaboration Platform Services</i>	239
<i>PLT002 Combined Federated Battle Laboratory Network (CFBLNet) Service for NATO Organisations</i>	243
<i>PLT003 Web Hosting Platform Service</i>	246
<i>PLT004 Service Oriented Architecture & Identity Management Service (SOA&IDM)</i>	249
<i>PLT006 Database Platform Service</i>	251
<i>PLT008 DevSecOps Service</i>	255
<i>PLT009 Electronic Definitive Media Library (EDML) Service</i>	263

<i>PLT010 Cloud Services Management and Integration (CSMI) Service</i>	<i>265</i>
<i>PLT011 Cloud Application Access (CloudApp) Service</i>	<i>269</i>
<i>PLT012 Maritime Command and Control Platform (MARC2P) Service</i>	<i>271</i>
<i>PLT013 NATO Integrated Secure Platform (NISP) Service</i>	<i>272</i>
<i>PLT014 Integration Tests Platform Service</i>	<i>275</i>
<i>PLT015 CQO Reference Platform Service</i>	<i>277</i>
SUBJECT MATTER EXPERTISE (SME) SERVICES	280
<i>SME002 Independent Verification and Validation for A2SL Service</i>	<i>281</i>
<i>SME003 Interoperability Verification and Validation Service</i>	<i>282</i>
<i>SME004 Provision of Subject Matter Expertise for the Federated Mission Networking (FMN) Framework</i>	<i>283</i>
<i>SME005.1 Acquisition Life Cycle Cost Estimating (LCCE) Service</i>	<i>284</i>
<i>SME005.2 Acquisition Software Intensive Project (SIP) Cost Estimating Service</i>	<i>285</i>
<i>SME005.3 Acquisition Cost Analysis (CA) Service</i>	<i>286</i>
<i>SME005.4 Acquisition Miscellaneous Cost Estimating & Analysis (MCEA) Service</i>	<i>287</i>
<i>SME007 Operational Application Support Service</i>	<i>288</i>
<i>SME008 Maritime Operational CIS Deployment and Recovery Service (MARCOM)</i>	<i>289</i>
<i>SME009 Provision of Subject Matter Expertise to support NCS as an Affiliate to Federated Mission Networking (FMN)</i>	<i>293</i>
<i>SME010 ACP127 Message Operator Service</i>	<i>294</i>
<i>SME012 VeVA CIAV Support</i>	<i>295</i>
TESTING SERVICES	297
<i>TST001 Independent Testing Service</i>	<i>298</i>
<i>TST002 Interoperability Testing Service</i>	<i>303</i>
APPLICATION SERVICES	310
<i>APP001 Approved Commercial-off-the-shelf Products Procurement Service</i>	<i>312</i>
<i>APP001A Supported Commercial-off-the-shelf (COTS) Business Applications</i>	<i>313</i>
<i>APP002 Shared Early Warning (SEW) Application Service</i>	<i>316</i>
<i>APP005 CBRN Application Service</i>	<i>319</i>
<i>APP006 Ballistic Missile Defence (BMD) System of Systems Management Service</i>	<i>324</i>
<i>APP007 TOPFAS Application Service</i>	<i>327</i>
<i>APP010 NIRIS Application Service</i>	<i>331</i>
<i>APP011 OANT Application Service</i>	<i>334</i>
<i>APP012 SMACQ Application Service</i>	<i>339</i>
<i>APP013 Data-centric Information Services Gateway (DISG) Application Service</i>	<i>344</i>
<i>APP015 JCHAT Application Service</i>	<i>346</i>
<i>APP016 JTS/FAST Application Service</i>	<i>349</i>
<i>APP017 Land C2 Application Service</i>	<i>352</i>
<i>APP018 Maritime C2 Application Service</i>	<i>356</i>
<i>APP021 JOCWatch Application Service</i>	<i>359</i>
<i>APP022 NCOP Application Service</i>	<i>362</i>
<i>APP023 NAMIS Application Service</i>	<i>366</i>
<i>APP025 Naval Mine Warfare Support Application Service</i>	<i>368</i>

APP026 Virtual Battle Simulation (VBS) Application Service	369
APP027 NATO Nuclear C2 Reporting Application Service	370
APP028 NATO Nuclear Planning Application Service	371
APP029 Military Message Handling Application Service	372
APP030 Tasker and Project Tracker Applications Service (TT+ and PITT)	375
APP031 Enterprise Document Management Application Service (EDMS)	376
APP032 Personnel Management Application Services	377
APP033 INTEL FS Application Service	384
APP034 Integrated Engineering Management (IEMS) Application Service	386
APP035 eLeave Application Service	388
APP036 Finance (FinS) Application Service	390
APP038 NATO Talent Acquisition Application Service	392
APP039 P3SM and Workflow Application Service	394
APP040 Enterprise Asset Management Application Service	396
APP041 Logistics Functional Area Services (LOGFAS) Application Service	398
APP043 Interactive Simulation Package (ISP) Application Service	404
APP045 SIGINT COINS Application Service	407
APP046 HMART Application Service	408
APP047 Open-Source Intelligence (OSINT) Service	411
APP048 Analyst Notebook (ANB) Application Service	413
APP049 Integrated Command and Control (ICC) Application Service	415
APP050 Air Command and Control Systems (ACCS) Application Service	419
APP052 Air Situation Data Exchange (ASDE) Gateway Service	424
APP053 Multi Airborne Early Warning Ground Integration Segment Site Emulator (MASE) Application Service	429
APP054 L16@29k Application Service	434
APP055 Core Geographic Information System (GIS) Application Service	437
APP056 ISR Collection Management Tool (ICMT) Application Service	439
APP057 INTEL FS SIGINT Capability (ISC) Application Service	441
APP058 Release Server (RS) Application Service	442
APP059 Joint Exercise Development and Management (JEMM) Application Service	444
APP060 - ISR Coalition Shared Data (CSD) & Imagery Intelligence (IMINT) Service	447
APP061 Air Command and Control Information Services (AirC2IS)	449
APP065 Joint Tactical Simulation (JCATS) Application Service	454
APP066 Joint Operational Simulation Application Service	456
APP067 RECCEN Application Service	458
APP068 Advisor Network (ANET) Application Service	460
APP069 Air Integrated Training Capability (ITC) Application Service	462
APP070 Training Objective Development and Management (TOMM) Application Service	465
APP071 Enterprise Business Application (EBA) Service	467
APP072 Core Financial System (CFS) Application Service	468
APP074 NATO Lessons Learned Portal (NLLP) Application Service	469
APP075 Electronic Warfare Functional Services (EW-FS) Application Service	471
APP076 Indications & Warnings (I&W) Application Service	474
APP078 ORION Space Domain Application Service	475
APP079 NATO Automated Biometrics Identification (NABIS) Application Service	477
APP081 Joint Advanced Distributed Learning (JADL) Application Service	479

APP082 Digital Emergency Alert Notification Service.....	481
APP083 Mission Planning Application Service for Dual Capable Aircraft.....	483
APP084 International Submarine Escape and Rescue Liaison Office (ISMERLO)	
Application Service.....	485
APP085 Housing Office Management Application Service.....	487
APP086 NATO Information Portal Application Service (NIP).....	489
APP087 CRC System Interface (CSI) Application Service.....	490
APP088 CINEMA (CSI Integrated Network Monitoring and Management Application)	
Service.....	496
APP091 CSI JREAP Router Application Service.....	500
APP092 Ship-Shore-Ship Buffer (SSSB) Application Service	503
APP093 Enterprise Architect Application Service.....	508
APP095 Agile Tools for task management - JIRA Software Service	510
APP100 Mobile Advisor Reporting Tool (MART).....	513
APP102 – REACT – PNT and NAVWAR Application Service	515
APP103 Business Process Management Application Service (BPM)	517
APP104 Medical Management Application Service.....	518
APP105 Exercise Portal Template Set (EXPOTS)	522
APP110 Information Environment Assessment (IEA)	524
APP113 Operational Application Support Service	526
APP114 Message Text Format Application Service.....	530
APP115 Joint Automated Deep Operations Coordination System	533
APP117 IOToolset Service.....	536
 SECURITY SERVICES.....	 540
SEC001 Security Accreditation Support Service.....	542
SEC004 Cyber Security Analysis Service.....	543
SEC005 NATO Cyber Defence Rapid Reaction Team	545
SEC006 Cyber Security Incident Management Service.....	547
SEC007 Cyber Security Monitoring Service.....	549
SEC009 Cyber Security Strategic Outlook and Outreach Service	551
SEC010 Cyber Security Information Sharing Service (CSISS).....	553
SEC011 Gateway Security Service	556
SEC012 CIS Endpoint Protection Support Service	559
SEC013 Crypto Compliance Support Service.....	561
SEC014 Crypto Management and Logistic Support Service	562
SEC015 Security Certificate Service.....	566
SEC019 Cyber Operations & Exercises.....	568
SEC022 Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security	
Service.....	570
SEC023 Penetration Testing Service.....	573
SEC024 Vulnerability Assessment Service.....	575
SEC025 Emission Security Service.....	577
SEC026 Attack Surface Reduction Service.....	578
SEC027 Continuous Security Posture Assessment Service	580
SEC028 Remediation Support and Coordination Service	582
SEC029 Cyber Security Platform and Infrastructure Service	585

<i>SEC030 Cyber Threat Hunting Service</i>	587
<i>SEC032 Adversary Emulation Service</i>	589
<i>SEC036 Cyber Portals Service (CyPS)</i>	593
LOGISTIC SERVICES	595
<i>LOG001 CIS Asset & Materiel Management Service</i>	597
<i>LOG002 Test Equipment & TEMPEST Level Testing</i>	601
<i>LOG003 Test and Evaluation of Electromagnetic Environmental Effects Service – 3rd Level</i>	605
<i>LOG004 Inspection of Electronic Devices for Security Measures</i>	607
<i>LOG005 Support to Exercises with Deployable CIS Equipment Pool (DCEP) Service</i>	608
OTHER SERVICES	611
<i>OTH002 Account Management Service</i>	613
<i>OTH003 AirC2 In Service Support Program of Work (ISS POW) General Support Service</i>	616
<i>OTH005 Training Capability Battle Lab Support Service</i>	617
TRAINING SERVICES	620
<i>TRA003 Education and Individual Training Availability and Maintenance (EIT A&M)</i>	621
NATO HQ ONLY SERVICES	622
<i>WPS001N NHQ Managed Device Service</i>	623
<i>WPS002N NHQ Identity Access Management Service</i>	627
<i>WPS009N NHQ Voice and E-mail Service</i>	630
<i>WPS016N NHQ Managed Mobility Service</i>	633
<i>INF001N NHQ Local Area Network (LAN) Service</i>	636
<i>INF004N NHQ Infrastructure as a Service</i>	639
<i>PLT006N NHQ Database Platform Service</i>	642
<i>APP001N NHQ COTS Applications</i>	645
<i>SEC001N NHQ Security Accreditation Support Service</i>	648
<i>SEC006N NHQ Cyber Security Incident Coordination Service</i>	651
<i>SEC007N NHQ Cyber Security Logging & Monitoring Service</i>	654
<i>SEC011N NHQ Gateway Security Service</i>	657
<i>SEC012N NHQ CIS Endpoint Protection Support Service</i>	661
<i>SEC014N NHQ Crypto Management and Logistic Support Service</i>	664
<i>SEC015N NHQ Security Certificate Service</i>	667
<i>LOG001N NHQ CIS Asset & Materiel Management</i>	670
<i>OTH001N NHQ Service Management and Control</i>	673
APPENDIX 1 – UNDERLYING SERVICES	677
<i>INF046 Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service</i>	678
<i>INF051 Enterprise Edge Service</i>	681
<i>INF063 Enterprise DataCenter LAN Service</i>	684

<i>SEC008 Cyber Security OPCEN Helpdesk Service</i>	<i>686</i>
<i>SEC020 Cyber Security Management Service.....</i>	<i>688</i>
<i>SEC101 – NCSC Coherence and Service Management.....</i>	<i>690</i>
<i>SEC102 – Centralised NCSC Level 1 Support (Remote)</i>	<i>693</i>
<i>SEC104 – Level 1 Support to NCSC Services (On-site)</i>	<i>695</i>
<i>TRA002 Education and Individual Training Delivery (EIT Delivery).....</i>	<i>697</i>
<i>SME005 Acquisition Service</i>	<i>699</i>
<i>SME022 Maritime Broadcast Operations Service.....</i>	<i>700</i>
<i>APP064 ITSM Toolset Application Service.....</i>	<i>702</i>
<i>OTH001 - Service Management and Control, Delivery Governance, Measurement, Reporting, and Integration Enabling Function.....</i>	<i>709</i>
<i>OTH004 DCIS – Management Support Service.....</i>	<i>718</i>
<i>WPS008 Enterprise Services Operations Centre.....</i>	<i>719</i>
ANNEX B - NON-STANDARD CUSTOMER SERVICES	723
<i>OTH008 Support to Customer’s Operational Mission and Business Continuity Plans (BCPs).....</i>	<i>724</i>
<i>OTH009 Enhanced Local Support.....</i>	<i>726</i>
<i>OTH010 Campus ICT Services.....</i>	<i>728</i>
<i>OTH011 Local Exercise Support.....</i>	<i>730</i>
<i>OTH012 Unique (local) Capabilities.....</i>	<i>732</i>
<i>SME006 Operational Analysis Service</i>	<i>734</i>
<i>SME011 Subject Matter Expertise and Technical Consultancy Service for NATO Software Tools (NST) Communications and Information (C&I) Partnership.....</i>	<i>737</i>
<i>SME013 Single European Sky Air Traffic Management Research (SESAR) Capability Implementation Study</i>	<i>740</i>
<i>FMN001 Provision of Support to the Federated Mission Networking (FMN) Framework.....</i>	<i>742</i>
<i>FMN002 Support NCS as an Affiliate to Federated Mission Networking (FMN).....</i>	<i>750</i>
<i>FDM001 Federated Network Design and Service Management - Vigilance and Enhanced Vigilance Mission Network (VeVA MN)</i>	<i>753</i>
ANNEX C – OTHER STANDARD PRODUCTS	760
<i>INF046 Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service.....</i>	<i>761</i>

Introduction to the NCI Agency Costed Customer Services Catalogue



This page is left blank intentionally

Due to large amount of changes in each version of the catalogue, the Record of Changes table below only lists the latest changes that are introduced in this current version.

10.2 Release Record of changes

Change category	Details
Modification of existing services	• WPS003 Enterprise User License Service Service Description updated • WPS014 Secure Voice Service minor corrections within SD • NDW002 NATO Digital Workplace Service (High Side) Available Networks updated • FMN001 Provision of Support to the Federated Mission Networking (FMN) Framework Service Description updated • FMN002 Provision of Support to the NATO Command Structure (NCS) as an Affiliate (NCSaaA) to the Federated Mission Networking (FMN) Initiative Service Description updated • INF046 Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service – part of the service moved to „<i>Underlying Services</i>” and part to „<i>Other Standard Products</i>” section • INF047 Firefly service flavour updated • OTH001 Service Management and Control, Delivery Governance, Measurement, Reporting, and ITSM Toolset Integration-Enabling Function – service description updated to reflect LEG008 mapping • OTH002 Account Management Service – service description updated to reflect LEG008 mapping • LOG001 CIS Asset & Materiel Management – service description updated to reflect LEG008 mapping • APP045 SIGINT Coins – correction of service rates • APP117 IOToolset Testing – correction of service rates for APP117-5B, APP117-5C, APP117-5D, APP117-5E, APP117-5F • APP102 REACT – PNT and NAVWAR Application Service - Service Rate corrected • SEC010 Cyber Security Information Sharing Service – service rate corrected • All SEC services were updated with Underlying services list • All NHQ service rates and service descriptions were updated according to BC decision

	• Further clarification of „<i>Underlying Services</i>” - Appendix 1 • Further clarification of Annex B Non-Standard Customer Services and Annex C Other Standard Products
New Services	• OTH008 Support to Customer's Operational Mission and Business Continuity Plans (BCPs) • OTH009 Enhanced Local Support • OTH010 Campus ICT Services • OTH011 Local Exercise Support • OTH012 Unique (local) Capabilities
Removed services	• APP037 Employee Performance Management Application Service removed from CCSC • Service Rate for INF020-15 HPE Server removed

10.1 Release Record of changes

Change category	Details
Modification of existing services	• APP060 ISR Coalition Shared Data (CSD) & Imagery Intelligence (IMINT) Service SD updated • APP041 Logistics Functional Area Services (LOGFAS) Application Service SD updated • OTH004 DCIS – Management Support Service moved to „<i>Underlying services</i>” Section • TST002 Interoperability Testing Service – Service Description updated • INF046 Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service – Service Description moved to Annex C-Other Standard Products and Service Rates moved to Other Standard Products Table • SME022 Maritime Broadcast Operations Service moved to Annex B-Non-Costed Customer Services • SEC036 Cyber Portals Service SD updated • INF013 NATO CIS (VLF) Mission Support for Submarine Operations Very Low Frequency (VLF) Broadcast Service SD updated, service name changed in Service Rates and Service Description • WPS002-1 User Account has been updated with footnote clarifying when it is part of NDW001/NDW002 and when it's requested separately

	WPS008 Enterprise Services Operations Centre (ESOC) Service, Service description updated according to review and agreement with CWG
New services/ flavours	- FDM001 Federated Network Design and Service Management - Vigilance and Enhanced Vigilance Mission Network SD add to CCSC 10.1 - Annex C – Other Standard Products has been created - SEC101 NCSC Coherence and Service Management, SEC102 Centralised NCSC Level 1 Support (Remote), SEC104 – Level 1 support to NCSC Services(On-Site) added to „Appendix 1 - Underlying Services” Section
Removed services	- APP009 Integration CORE (INT-CORE) Application Service removed from Catalogue and Service Rates according to ISNOR/BC decision - APP019 White Shipping Picture Application Service removed from Catalogue and Service Rates according to ISNOR/BC decision - APP108 NMAD Application Service CORE (INT-CORE) Application Service removed from Catalogue and Service Rates according to ISNOR/BC decision - INF002NLI - NGCS Legacy Infrastructure PoP removed from Catalogue and Service Rates according to ISNOR/BC decision - INF015-2 BRASS IP Enhanced System (BRIPEs) removed from Catalogue and Service Rates according to ISNOR/BC decision - INF022-1 1st Generation DSGT removed from Catalogue and Service Rates according to ISNOR/BC decision - OTH007 Operational Asset Management and Logistics removed from Catalogue according to ISNOR/BC decision - NDW007 NATO AI Chatbot removed from Service Rates according to ISNOR/BC decision - APP006, APP043, APP053, APP054, APP069, APP083, OTH003, PLT013, INF028, INF034 removed from Service Rates Table

10.0 Release record of changes

Change category	Details
Modification of existing services	• Appendix 1 listing Underlying Services and their respective service descriptions has been created. • Annex B for Non-Costed Services has been created. • Sentence defining <i>Underlying Services</i> has been added in The Catalogue Section. • New Service Field <i>Underlying Services</i> with clarification of which underlying services are underlied to each service has been added to multiple services. • Under the CCSC Service Portfolio Grouping Section new Testing Services have been added. • Service Rates and service descriptions for NDW Services have been added and WPS001 removed (transitioned to NDW001, NDW002 and NDW003). • The following sentence has been removed from all SEC services: <i>"This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally"</i>. • SEC001 Security Accreditation Support Service; SEC005 NATO Cyber Defence Rapid Reaction Team; SEC009 Cyber Security Strategic Outlook and Outreach Service; SEC023 Penetration Testing Service; SEC024 Vulnerability Assessment Service descriptions have been modified to better explain the deliverables as part of the cybersecurity working group endeavours. • SEC027 Continuous Security Posture Assessment Service has been modified to reflect the addition of a new service flavour (SEC027-6: Active Directory Security Assessment). • SEC028 Remediation Support and Coordination Service and SEC032 Adversary Emulation Service Description have been updated as per the Cyber Security Working Group feedback. • APP006 Ballistic Missile Defence (BMD) System of Systems Management - the wording

	<i>“Underlying Services”</i> has been renamed to to <i>“Other Supporting Services”</i>. • The following services have been updated to reflect the new costing model: APP001 Approved Commercial-off-the-shelf Products Procurement Service, APP002 Shared Early Warning Service, APP005 CBRN Application Service, APP007 TOPFAS Application Service, APP010 NIRIS Application Service, APP011 OANT Application Service, APP012 SMACQ Application Service service, APP015 JCHAT Application Service, APP016 JTS/FAST Application Service, APP017 Land C2 Application Service, APP018 Maritime C2 Application Service, APP021 JOCWatch Application Service, APP022 NCOP Application Service, APP029 Military Message Handling Application Service, APP032 Personnel Management Application Service, APP041 Logistics Functional Area Services LOGFAS APP068 Advisor Network (ANET) Application Service have been updated to reflect the new costing model, APP093 Enterprise Architect Application Service, APP104 Medical Management Application Service. • APP047 Allied Command Open Source Application Services – renamed to Open-Source Intelligence (OSINT) Service with updated service description. • APP060 ISR Coalition Shared Data (CSD) Service – renamed to Imagery Intelligence (IMINT) Service with updated service description. • APP064 ITSM Toolset Application Service Service Description has been moved to the Underlying Services – Appendix 1. • APP075 Electromagnetic Warfare Functional Services (EW-FS) Application Service – updates to value proposition, service features, service flavors, service restoration and the addition of service ordering and request. • APP078 ORION Space Domain Application Service – updates to the service description and service flavours. • APP081 Joint Advanced Distributed Learning (JADL) Application Service – updates to service support levels and addition of service ordering and request. • WPS002 Enterprise Identity Access Management Service has been updated.

	• WPS008 Enterprise Services Operations Centre Service description updated and moved to Underlying Services – Appendix 1. • INF004 Infrastructure Virtualization Service, INF006 NATO Enterprise Directory Service (NEDS), INF015 Broadcast, Maritime Rear Link and Ship-Shore (BRASS) STIV RMD service, INF020 DCIS – Deployable CIS Equipment Pool (DCEP), INF035 DCIS – Deployable CIS Nodes Service for Land Based Users (LBU), INF036 DCIS – Deployable SATCOM Service, INF038 DCIS – Deployable Nodes Anchor Service descriptions have been updated. • TRA002 Education and Individual Training Delivery (EIT Delivery) was moved from Catalogue Services to the Underlying Services - Appendix 1. • INF051 Enterprise Edge service description updated to reflect NPCL-related flavours. • SME004 Provision of Subject Matter Expertise for the Federated Mission Networking (FMN) Framework – Service Description replaced by sentence about retirement of the service and replacement by FMN001 which has been added to the none costed services annex. • SME006 Operational Analysis Service - moved to Appendix 2 Non-Costed Customer Services. • SME008 Maritime Operational CIS Deployment and Recovery Service updated. • SME009 Provision of Subject Matter Expertise to support NCS as an Affiliate to Federated Mission Networking (FMN) - Service Description replaced by sentence about retirement of the service and replacement by FMN002 which has been added to the none costed services annex. • SME011 Subject Matter Expertise and Technical Consultancy Service for NATO Software Tools (NST) Communications and Information (C&I) Partnership and SME013 Single European Sky Air Traffic Management Research (SESAR) Capability Implementation Study have been moved to Non-Costed Customer Services annex. • SME022 Maritime Broadcast Operations Service description has been updated. • TRA002 Education and Individual Training Delivery (EIT Delivery) and TRA003 Education and Individual Training Availability and

	Maintenance (EIT A&M) service descriptions have been updated. • PLT008 DevSecOps Service and PLT010 Cloud Services Management service descriptions have been updated. • WPS007 Print/ Scan/ Copy Service, WPS012 Workstream Collaboration Service; WPS014 Secure Voice Service; WPS016 Enterprise Managed Mobility Service descriptions have been updated. • PLT001 Information Sharing and Collaboration Platform Services, PLT003 Web Hosting Platform Services, PLT004 Service Oriented Architecture & Identity Management Service (pipeline) and PLT006 Database Platform Service have been updated. • OTH001 Service Management, Delivery, Measurement, Reporting, and Integration Enabling Service has been moved to Underlying Services – Appendix 1.
New Services/ Flavours	• TST001 Independent Testing Service and TST002 Interoperability Testing Service. • APP009 Integration CORE (INT-CORE) Application Service. • APP019 White Shipping Picture Application Service. • APP105 Exercise Portal Template Set (EXPOTS). • APP108 NMAD Application Service. • APP113 Operational Application Support Service replaced SME007. • APP114 Message Text Format (MTF) Application Service. • APP115 Joint Automated Deep Operations Coordination System added as a pipeline service. • APP117 IOToolset Service. • INF015-2 BRASS IP Enhanced System (BRIPEs). • INF055 DCIS - Mission Adaptable Reference System (MARS) Service. • INF056 DCIS Nodes – Deployable CIS Nodes for Maritime Based Users (MBU). • INF060 DCIS General Purpose Deployable CIS. • New pipeline service INF062 NS Mobility NSMOB (HERMES) added.

	• INF063 Enterprise DataCenter LAN Service added as underlying service. • SEC035 Cyber Functional Area Service and SEC036 Cyber Portals Service have been added. • NDW005 Digital Events Service; NDW006 Information and Knowledge Management Applications and NDW007 NATO AI Chatbot have been added. • OTH007 Operational Asset Management and Logistics has been added under Appendix 1 - Underlying Service section. • NEW section for NATO HQ Only Services has been created and service descriptions have been added.
Removed Services	• The following services have been removed: NDW004 Hybrid Work Environment - Audio-Visual Services; WPS004 E-mail Service; WPS005 Instant Messaging and Collaboration Service; SME001 Chief Quality Office Subject Matter Expertise Service; SME002 Independent Verification and Validation for A2SL Service Description has been retired and replaced by TST001; SME003 Interoperability Verification and Validation Service Description retired and replaced by TST002; SME005.1 Acquisition Life Cycle Cost Estimating (LCCE) Service, SME005.2 Acquisition Software Intensive Project (SIP) Cost Estimating Service, SME005.3 Acquisition Cost Analysis (CA) Service and SME005.4 Acquisition Miscellaneous Cost Estimating & Analysis (MCEA) have been retired; SME010 ACP127 Message Operator Service Service Description has been retired and became a flavor of APP029; SME012 VeVA CIAV Support Service has been retired and replaced by TST002; SME014 Provision of SME to Support the Governance and Management of the VeVa Mission Network; SME017 NATO Collaboration Solutions Expertise Service; SME021 C2 Data Integration and Management Service; APP014 NMRR-VMS Application Service; APP089 Tasking, EXploitation and Assessment System (TEXAS); INF008 DCIS – DragonFly Service; INF009 DCIS – Limited Interim NATO Response Force (NRF) CIS-Expansion (LINC-E) Service; INF010 DCIS – Communications Gateway Shelters (CGS) Service; INF017 DCIS – In-Theatre Mobile CIS Detachment (IMCD) Service;

	INF018 DCIS – Mini Point of Presence (Mini-PoP) Service; INF019 DCIS – Theatre Liaison Kit (TLK/ILK) Service; INF021 DCIS – Third Generation Transportable Satellite Ground Terminal (TSGT) and Upgraded Transportable Satellite Ground Terminal (UTSGT) Service; INF022 DCIS – Deployable Satellite Ground Terminal (DSGT) Service; INF024 DCIS – High Frequency (HF) Service; INF025 DCIS – Deployable Line of Sight (DLOS) Service; INF026 DCIS – Deployed Operational Gateway (DOG) Service; INF027 DCIS – Mission Preparation Centre Service; INF032 DCIS – Small Deployable Military Bandwidth SATCOM Terminal (DMBST) Service; INF039 E-Mail Federation Service; INF044 SEMARCIS/SEMARCOM Deployable Maritime CIS; INF045 DCIS Remote Network Module (RNM); PLT007 DCIS – Afloat Command Platform (ACP) Service; PLT005 Active Directory and Federation Service; PLT012 Maritime Command and Control Platform (MARC2P) Service; SEC017 Crypto Assessment Support Service; SEC018 Cyber Security Project Management Service; SEC021 DCIS – Signal Support Group (SSG) Service. • SEC008 Cyber Security OPCEN Helpdesk Service and SEC020 Cyber Security Operations Management Service have been moved to Underlying Services – Appendix 1. • APP030 TT+ and PITT, APP031 EDMS, APP086 NIP services have been retired and replaced by NDW006.

Retired services/flavours currently supported

This section includes the services/flavours which have been recently retired and are not available for ordering in this Catalogue release. However, they are still supported for the previous year's quantities, until customers transition to the recommended alternatives or the life expectancy of the service /flavour components reaches its end.

WPS007-2 NONO (NATO Owned NATO Operated) Printer - a device suitable for office or small workgroup environments. It supports up to 5k prints per month, enables up to A4 printing in colour and B/W, and may print up to 20 pages per minute in B/W and 20 pages per minute in Colour.

This flavour is not available anymore for ordering and the alternative is one of the listed Flavours available for ordering (WPS007-1 products). In order to transition to the alternative

option, customers need to raise a CRF and the deadline is approximately 14 weeks (including TEMPEST).

Quantities listed in 2022 SLAs/SSPs will be supported until the device has reached its supported life expectancy age (4 years).

WPS016-5 Multi-Factor Authentication Token for Non-managed Devices – This option enables users to access OWA (Outlook Web Access), VDI (Virtual Desktop Infrastructure) or other corporate NU resources made available via the public internet and requiring authentication, through the use of unmanaged (non-NATO) client devices. This One-time-password (OTP) solution - token - is part of the two-factor authentication mechanism required for access.

This flavour is not available for new quantities ordering. Quantities listed in 2022 SLAs/SSPs will continue to be supported.

References

- A. C-M(2012)0049, Charter of the Communications and Information Organisation (NCIO), 14 Jun 2012;
- B. PO(2015)0394, NCI Agency Customer Funding Regulatory Framework, 7 July 2015;
- C. AC/337(FC)N(2017)0025 (INV), Report on Agency Service Costing/ 2018 Service Cost Calculation Methodology, 25 April 2017.

The Catalogue

The NCI Agency Costed Customer Services Catalogue provides a unique and standardised list of Services which are offered to the customer in support of their achievement of specific business outcomes and objectives. The NATO enterprise is complex and extensive; comprised of many different geographically dispersed customers and entities, spanning a wide spectrum of requirements and needs. The NCI-Agency Costed Customer Services Catalogue reflects this complexity by providing a wide range and variety of services, service variations (flavours), value added services, and products. As such, the Costed Customer Services Catalogue forms a true representation of the diverse needs of customers.

The Catalogue constitutes a living document which adapts and matures as customer requirements evolve and change over time. Maintaining a proper alignment between both services and customer requirements is a key principle which enables the NCI Agency to support and add value to customer business. This catalogue has been build and structured on the basis of a customer-centric approach and in accordance with standards and definitions in industry best practice.

The NCI Agency Costed Customer Services Catalogue constitutes primarily a list of Services. However, many of the services in the catalogue can also be offered in the form of a product. To this end, the Agency enclosed a supplemental product catalogue which complements the service catalogue. The product catalogue allows the NCI Agency to remain flexible towards the needs and objectives of customers. Moreover, it provides the means to cater to a larger and more distinct group of customers who, either for technical reasons or business motives, are not able to consume services. The NCI Agency Costed Customer Services Catalogue is

therefore comprised of two distinct but paired catalogues, i.e. the Services Catalogue and the Products Catalogue. This introductory note explains the concepts of “services”, “products” and “value added services” for the convenience and understanding of the customer in the use of this Catalogue.

For transparency, Appendix 1 of this document provides an overview of the underlying services, including their service descriptions. Although underlying services are not delivered directly to customers as part of the CCSC, they are essential in enabling and supporting the delivery of customer-facing services. The costs associated with these underlying services are fully incorporated into the pricing of the customer-facing services.

The NCI Agency Costed Customer Services Catalogue also includes Annex B, which is referring to Non-Standard Customer Services. Non-Standard Customer Services are services, which don't have standard scope and thus standard rate and hence not costed in costed customer service catalogue. They're subject to individual pricing.

The NCI Agency Costed Customer Service Catalogue also includes Annex C, which is referring to Other Standard Products. Other Standard Products are products which don't refer to an annual O&M rate, however they have one time cost (per requirement) which is same for all customers.

Service

ITIL defines a service as a set of related functions provided by IT systems in support of one or more business areas, which in turn may be made up of software, hardware and communications facilities, perceived by the customer as a coherent and self-contained entity. An IT Service is based on the use of Information Technology and supports the Customer's Business Processes. Additionally, ITIL specifies that an IT Service is made up from a combination of people, processes and technology and should be defined in a Service Level Agreement¹. In essence, a service delivers an intangible benefit², either in its own right or as a significant element of a tangible product. For example, the provisioning of the NCOP functional application service provides customers with an increased situational awareness on the battlespace, increased collaboration and ultimately improved military operations. As opposed to products, the concept of providing a service is not limited to the delivery a specific tangible or intangible system, but rather the provisioning of a whole set of logically related processes, activities, infrastructure, technologies, which in combination with specific skills and knowledge, is able to add value by facilitating customer's business outcomes and goals. Therefore, when we refer to services, we do not just include the provisioning of a specific solution or product, but in addition, include all activities related to the deployment, configuration, management, maintenance and operation. Together, as a packaged whole, they denominate and qualify the concept of a Service. Ultimately, a service provides a level of abstraction, which allows the customer to focus on outputs and outcomes without incurring any intrinsic risks related to the operation and maintenance of the service. When services are

¹ ITIL V3 definition of a Service.

² These benefits (outcomes) are generally difficult to measure and quantify and as such are mostly referred to as “intangible”.

priced¹ they incorporate all cost elements which are related to the provisioning of a service (operation and maintenance), both in terms of manpower and external CIS costs.

Services within the NCI Agency Costed Customer Services Catalogue are categorised into 9 different groups, commonly referred to as “Service Portfolio Groupings”, these are:

- Workplace Services
- Infrastructure Services
- Platform Services
- Subject Matter Expertise Services
- Application Services
- Logistic Support Services
- Security Services
- Training Services
- Other Services

Service Portfolio Groupings

Services within the NCI Agency Costed Customer Services Catalogue are categorised into 9 different groups, commonly referred to as “Service Portfolio Groupings”. These are:

- **NATO Digital Workplace Services:** This is a new portfolio group that captures the services which are part of the NATO Digital transformation roadmap (#One NATO) initiative which is supported by OCIO strategic initiatives.
- **Workplace Services:** Workplace Services comprise of the basic CIS services that users typically need in their workplace in order to perform their day-to-day business activities, regardless of their job specialization. The majority of NCI Agency’s customer base users consumes these services.
- **Infrastructure Services:** Infrastructure services deliver the underlying data centre and hardware, software, network, storage and backup functions required for the existence, operation and management of an enterprise ICT environment.
- **Platform Services:** Platform Services provide a package of middleware allowing users to develop, run, and manage applications or data sets without the complexity of building and maintaining the underlying infrastructure. Platform Services deliver the infrastructure and middleware components that enable IT administrators and end users to build, integrate, migrate, deploy, secure, and manage mobile and web applications. Platform Services enable delivery of cost-effective, fully managed operating platforms with expanded, inheritable, and NATO recommended security controls.
- **Subject Matter Expertise Services:** Services provided through a Subject Matter Expert (SME), an individual who is considered an expert on particular subjects, or flagged as an expert in a piece of management software or other technology. The subject matter expert has a particular territory in which he or she has demonstrated above-average knowledge or experience.

¹ NCI Agency is costing or pricing the Services in accordance with the Customer Funding Regulatory Framework.

- **Application Services:** Software with functionality delivered on-demand to subscribers, which includes web based or client-server applications. Application Services enable customers to collect, manage, present, and distribute information in support of specific Community of Interest (COI) processes. They comprise of entire enabling technology required by any kind of NATO organisations to support a wide spectrum of their business activities.
- **Logistic Services:** The services that support the availability and continuing operation of an asset or piece of equipment in accordance with established standards. Usually, these services entail supply, maintenance, and transportation activities, but may be extended beyond this scope (e.g. calibration, equipment testing, etc.).
- **Security Services:** Services ensuring adequate security of the systems or of data transfers (network and information system security). The Security Services are responsible to NCI Agency for providing support to the development and implementation of Lifecycle security risk management services for NATO ICT IT, IT security related policy and strategy, Leadership in the development of new capabilities and innovation. The security services are focused on to prevent, detect, respond, and recover any IT security related incidents. CIS Security Capabilities provide the secure environment for handling information by CIS components, systems, services, and resources.
- **Training Services:** Services dedicated to educating users on CIS-related topics; designed to help trainees acquire certification in specific areas.
- **Testing Services:** This group of services provides on-demand testing of software, hardware and ICT systems. This ensures that applications, systems and their services meet operational and interoperability requirements, standards, and user expectations before deployment in operational and mission networks. This service group enables organizations to leverage specialized testing expertise, tools and infrastructure to provide the required assurance for applications and systems. As such, it assures that the associated and identified potential products risks are timely mitigated, preventing any negative impact on the operational challenges. By making timely use of these services, the number of undetected hardware and software defects found on operation and their impact are drastically reduced.
- **Other Services:** Catalogue services that cannot be placed in any other specific Service Portfolio Grouping.
- **NATO HQ Only Services:** Catalogue services available only for NATO HQ.

Service Delivery Lifecycle Stages

A service delivery lifecycle typically follows 3 stages from a business point of view: Service Initiation, In-Service-Support, Lifecycle Refresh. The separation of the lifecycle into these 3 stages facilitates the transparency and management of the different nature of deliverables, time frames and costs that are applicable to each stage. Due to this difference of nature, each stage also has its corresponding separate service rate.

The lifecycle stages and corresponding service rates are explained further below:

1) Service Initiation Rate

Service Initiation is the first stage of the service delivery which corresponds to the one-time cost involved in order for the NCI Agency to set the service up and running.

Service initiation rate covers the cost of procurement of the service assets, delivery to the user location and the initial installation effort for one unit of service requested.

When a customer requests a service for the first time, the one-time Service Initiation Rate is the first rate to be applied. Once the service is initiated, it moves into the next stage: in-service-support.

2) In-Service-Support Rate

In-service-support stage is where service operations and maintenance (O&M) activities are performed by the NCI Agency in order for the service to continue delivering its proposed value.

The in-service-support stage of a service is meant to be long term, and this stage is managed in repeating annual Customer Service Agreements with the customer. In-Service-Support Rate thus corresponds to the annual rate entailing the NCI Agency manpower support costs and the annual fee that the Agency pays to external/industry contracts (license maintenance, 3rd party support, spare parts etc.) for ensuring the seamless continuation of the service provision.

3) Service Lifecycle Refresh Rate

This is the last stage of the service delivery, where the main assets of the service reach the end of their lifecycle and must be replaced for seamless continuation of service delivery. Typically the lifecycle duration is stated in the Customer Service Agreements per service. The service lifecycle refresh rate corresponds to the one-time effort to replace these assets that are at the end of their lifecycle.

The NCI Agency is working towards offering a standard service rate for all applicable services in the Costed Customer Services Catalogue and for each stage in the service delivery lifecycle. The Service Rates section of this Costed Customer Services Catalogue lists the standardised service rates the Agency currently has, with the clear indication of what stage in the service delivery lifecycle the rate applies to. Where the Agency does not yet have a standard service rate, a custom-calculation of the service rate is applied.

Product

As opposed to services, Products are tangible and discernible items, which are delivered as physical assets or intangible assets. While a product is something that can be quantified, a service is less concrete and is the result of the application of skills and expertise towards an identified and specific objective. Most commonly products are delivered in the form of an unmanaged device (e.g. Laptops, desk computers, phones, smartphones, etc.) or software application (e.g. functional applications and specialist applications). Contrary to services, these products will be delivered in a standalone state, without any support in terms of installation, configuration, maintenance and operation. Moreover, especially for functional applications, where the underlying infrastructure is not owned or operated by NCI-Agency.

The price for a product therefore equates to its base cost of acquisition. In some instances where standardisation is of no or little importance, i.e. COTS Software, customers are free to purchase the product via their own channels.

Value Added Service

By themselves, products do not satisfy any specific and immediate business need or objective. Only when deployed, configured, maintained and operated they can be used in support of certain business activities. In order to cater for the eventuality where such additional activities are required, NCI-Agency has created the concept of Value Added Services. As the name suggest, value added services enhance and complement specific products, and in some instances services⁴. The product in combination with all or some of its value added services therefore equates to its service counterpart¹. From a pricing perspective, value added services are mostly, if not exclusively, comprised of costs, which are related to human resources. The cost of a value added service is therefore dependant on the number of manpower units (FTE) that are needed to execute and deliver specific activities. Value added services are referred to as services because they exclusively consist of the delivery of specific NCI-Agency expert skills and knowledge. They are however quite distinct from the services which were defined earlier. Therefore, the NCI-Agency Customer Service Catalogue will group all of the value added services in a separate list in the future.

Value added services can be provided for a number of areas or activities:

- Installation & Configuration
- Release Management (Patch and version releases)
- In-Service-Support (Level 1,2 and 3)
- Mentoring
- Training
- Project Support
- Auditing

Service & Product Attributes

The NCI Agency Costed Customer Services Catalogue adopted a standardised template for describing services and products. A description comprises a specific set of attributes, which define and qualify the service or product. The description templates have been designed from a business- and customer-centric point of view. The following table lists and defines all attributes valid for NCI Agency Product and/or Service.

¹ It should be noted that in some instances, as for example with mentoring and training which qualify as “value added service”, customers who have opted for the service are still eligible to purchase these value added services.

#	Attribute name	Attribute Description
1	Service/Product ID code	6 character code, which uniquely identifies a service or product; customers can use this code to refer to specific service or product; provided by NCI Agency Service Portfolio / Service Catalogue Management (COO BPM SPCM).
2	Service/Product Name	Name designating the service or product, as proposed by the Service Owner.
3	Portfolio Group	Indicates the Service Portfolio Group to which the service in question belongs: Application, Infrastructure, Platform, Subject Matter Expertise, Security, Training, Workplace, Other.
4	Service/Product Status	Indicates the Portfolio status of the Service or product, i.e. "Pipeline", "Available" or "Retired". Pipeline services are planned to become available, and may even be partially available to specific customers. Available services are offered to customers as defined in the Catalogue. Retired services are not available for ordering, but they might be fully or partially supported for a specific period of time after being announced as retired through the Catalogue.
5	Service/Product description	Describes the service or product from a non-technical perspective.
6	Value Proposition	Explains in business terms how a service or product supports specific business processes and as such facilitates specific business outcomes and objectives.
7	Service/Product Features	Lists and describes the features of the service or products. Complements the service description.
8	Service/Product Request	Describes the procedure, which is required for customers to request the service or product. Describes the means by which customers can report incidents and problems related to the use of the service or product.
9	Service/Product Flavours	Describes the different variations in which a service or product can be offered.
10	Available Networks	Lists the security environments in which the service or product is available, i.e. NU – NU – NS – MS, on which the service can be delivered.
11	Service/Product Prerequisites	Lists the services, which are required beforehand in order to consume the service in question. The Customer needs to ensure that the prerequisite service are in place. For products, this section will be dedicated to system prerequisites.
12	Standard Service Support levels	Details the availability target for the service, i.e. the time the service is available to the customer considering the potential downtime of a service. This figure does not include any maintenance activities. Service Availability Target is expressed in terms of the minimum "Monthly Uptime Percentage" time frame. Percentage availability is calculated by the following formula: $\% \text{ Availability} = 100 \times (\text{Available Minutes}^* - \text{Downtime}) / \text{Available Minutes}$ <i>*Minutes available during agreed reporting period excluding planned maintenance minutes</i>

#	Attribute name	Attribute Description
		This section also details the restoration time for a service, i.e. the maximum time which is needed to restore the service in the eventuality of a major or critical incident.
13	Service Reporting	Details the standardised service reporting which is provided as a deliverable of each service
14	Support Hours	Details the times during which helpdesk support (including level 2 and 3 support) is available for the customer.
15	Service/Product Cost	Describes the unit of measure (service unit) ¹ used in the calculation of the service price/rate. Provides reference for price detail, or describes specific application of the service rate, where applicable. This attribute will only detail the base acquisition price for products.

Unless otherwise specified in a specific service definition, the following attributes are equally valid for all services in the Catalogue:

Service Status: Available

Service Support levels and Prioritization: All services have default P4 priority. Any change of priorities is subject to specific stipulations of the respective service definition within this Catalogue and relevant service provisioning agreements (Service Level Agreements and/or Service Support Packages).

The service rates reflect the prioritisation requirement of the services based on the default prioritisation in the CCSC plus the ACO ABIPAT tables in SLAs.

Support Hours:

- Centralized Service Desk specialist agents are available Mon-Thurs 06.00-22.00 CET, Fri 06.00-20.00 CET. Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.
- Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Requests

¹ Currently, the NCI Agency applies specific unit of measure for only a portion of the overall service portfolio. These are referred to as “unitized” services, as opposite to majority services that are “non-unitized”, and have the unit of measure defined as 1. Non-unitized services are priced per total cost of the specific service delivery, and normally funded by one funding mechanism (one service provisioning agreement). In cases where those services are provided to both External and Internal Customers, price for each specific service delivery other than the main one needs to be separately defined in the process of the service provisioning agreement development. Prices for unitized services are equally applied per unit of measure for all customers.

- **New Service Request:**

Please complete [Customer Request Form](#) and contact NCI Agency, as defined within the form.

- **Incident/problem reporting:**

Contact Centralized service desk: 626 3177 (NCN) or the commercial numbers:
 Belgium +32 65 44 3177,
 Netherlands +31 70 374 3177,
 Italy +39 081 721 3177,
 Germany +49 282 4978 3177,
 NATO HQ +32 02 707 5858.

NCI Agency Education and Training Services

NCI Agency provides a comprehensive catalogue of NCI Agency Education and Training Services covering in the entire spectrum of NATO-Specific C4ISR and Cyber, including user, administrator and technical training, as well as courses for military and civilian staff working in more general Communications and Information Systems posts. The Catalogue also explains how to obtain services, the procedure for seat allocation as well as the pricing policy and prices for many of the courses. The catalogue is a living document, as the Agency dynamically adjusts its course offerings to accommodate new systems being delivered, systems being phased out, new versions and changing customer requirements. The catalogue and pricing information can be found at www.ncia.nato.int/training.

NCI Agency Services not covered by the Costed Customer Services Catalogue

The Agency aims to offer its services, to the greatest extend, in a standardized manner via the Agency Costed Customer Services Catalogue (CCSC), where each Service has a standard scope of service provision and Standard Service Rate (where applicable). The use of the CCSC services provides both the customers as well as the Agency elements a pre-defined standard understanding of the scope, expectations and deliverables for the customer needs.

However, in cases where a local support is required by a customer that cannot be attributed to a CCSC Service, the Agency provides the flexibility to offer these service offerings through a group of what is called: 'Non-Catalogue Services'. Agency provides a variety of support for its customers under the scope of 'Non-catalogue service', however for practicality, the Agency groups these services under one of its **9 Non-Catalogue Service** titles (please see table below) during reporting. In that regard, these 9 service titles rather represent a Service Group, rather than a standard offering. Because the scope of each service for these services is different for each customer, the specific service deliverables for these services should be documented in the corresponding Service Agreements.

The management and provision of these Non-Catalogue Services are handled by local Agency elements. Financially, the cost of these services are custom calculated and agreed during the Service Agreement negotiations between the customer and Agency.

In the table below, you may find an explanation of what each Non-Catalogue Service, or service group can entail.

NCI Agency Non-Catalogue Services		
Title	Service ID	Description
Local Audio / Video Support Service	LEG001	Corresponds to local audio visual support that is not part of a standard service offering in the CCSC. May include but is not limited to operation and maintenance of projection systems, TVs, IPTV, portable audio systems, large screen displays (ex Videowall) and smart boards.
Local Internet Access Service	LEG002	Corresponds to locally managed fixed or wireless internet access services that are outside the scope of the standard service offering (Enterprise Internet Access Service – INF003) found in the CCSC.
Local Transmission Service	LEG003	Corresponds to locally managed and supported transmission lines for connecting NATO networks to/from the site that are not covered under the CSLA funded transmission services (INF014)
Local Applications Service	LEG004	Corresponds to any local application maintenance and support requirement that is not part of a standard service offering in the CCSC, where the application will be locally managed.
Local CIS Security Service	LEG005	Corresponds to local CIS Security support requirement that is not part of the centralized Agency service offerings or where the customer requires local SME and consultancy support on matters related to CIS Security.
Local Radio Communication Service	LEG006	Corresponds to local Radio Communication requirements (like first responder radio equipment) that is not part of a standard service offering in the CCSC.
Local SME / PoW Service	LEG007	Any local Subject Matter Expertise requirement that customers that is not part of a standard service offering in the CCSC. The scope of services ranges from providing SME and consultancy services to supporting customers on PoW related activities such as Small Value Sales.
Local Other Service	LEG008	Any local support requirement that doesn't fall under neither of the categories above.

Local User Training Service	LEG009	Local training requirements of the customer that are beyond the scope of the NATO CIS School that is covered in the CSLA.

Costed Customer Services Catalogue - Definitions

This page is left blank intentionally



NATO Digital Workplace Services

NDW001 NATO Digital Workplace Service (Low Side)

Service ID: NDW001

Service Name: NATO Digital Workplace Service (Low Side)

Portfolio Group: NATO Digital Workplace Services

Service/Product Status: Available

Service Description: The NATO Digital Workplace Service is the work environment for NATO staff. NDW001 has all the features and functionalities required in NATO's Digital Workplace, so Staff can connect, communicate and collaborate in an effective way taking Staff Productivity and Enablement to the next level.

Value Proposition: NDW001 provides comprehensive and mutually complementary set of features and functionalities as one cohesive intelligence to the NATO Enterprise. Unified set of features and functionalities will enable Staff to easily connect, communicate and collaborate within and across Entities on NU (NPCL) network.

NDW001 not only simplifies the standard service offerings but also unites the NATO Enterprise by ensuring that previously fragmented features and functionality are available to all NATO Enterprise Staff.

The availability of a NATO Digital Workplace with common set of features and functionalities allows digital and cloud-native business process transformation, end-user Digital Enablement (adoption, digital dexterity ¹& satisfaction) and drives further the NATO Digital Transformation.

Service Features: The Service provides the following features and functionalities:

- Computing Platform (Operating System) depending on the selected hardware (NDW003);
- Operating system and baseline application management (patching, upgrades, etc.)
- Mandatory Security Components;
- Approved hardware authentication token (e.g. smartcard, hardware key);
- Digital #OneNATO name (ENTITY | LASTNAME Firstname | *Optional Fields*);
- Unified NATO identity (@ENTITY.nato.int or @nato.int) with one personal mailbox;
- Digital Signature (hardware authentication token);
- Personal Storage Space (Microsoft OneDrive, 20GB per user);
- Collaboration (Microsoft Teams for instant messaging, email, Polycom for NCS users);
- Integration with NCN and commercial (fixed and mobile) telephony systems*;
- Content Creation (Microsoft Office Suite, Adobe Acrobat Reader);
- Access to digital enablement content (training material, videos, etc.);
- Packaging of the mandatory software present on every devices (Enterprise Candidate Applications);
- Distribution to end users, support for installation of software applications procured through APP001 service and/or available on A2SL (software license costs are not included and has to be requested via APP001 service separately).

¹ Digital Dexterity is the beliefs, the mindsets and behaviors, that accelerated digital business transformation (Harvard Business Review 2021)

***Note:** The integration enable users to use their NCN extension number (purchased with WPS009) and/or their commercial mobile number (purchased with WPS016) with collaboration tools installed on the device (MS Teams). The feature is only available when IP based centralised telephony infrastructure is available.

Service Ordering and Request: The new service instances are requested by submitting a Customer Request Form (CRF). After a service is initiated, the in-service support phase for the service is managed through annual Service Agreements with each customer. The service fee for this service is charged to each Agency customer directly, meaning the service charges are not covered by the NATO central funding channels for NATO, therefore each customer requests/orders this service directly themselves.

For IT Incidents, Request for Information (RFI) and Service Requests (SR) regarding this service, the Enterprise Service Operations Centre (ESOC) is the NCI Agency's Single Point of Contact (SPOC) for all eligible Customers and Users.

Service Flavours: NATO Digital Workplace Service (Low Side) flavours:

NDW001 comes only in one service flavour, which is covering the low side (NU). The equivalent service for higher content classification can be found under NDW002 NATO Digital Workplace Service (High Side).

Available Networks:

The Service is available on NATO Unclassified NCIA-managed CIS.

Service pre-requisites:

NDW003 Personal Workspace - Managed Device Service (a maximum number of devices as covered via WPS003 Enterprise User License Service)
WPS003 Enterprise User License Service
SEC015 Security Certificate Service

Underlying Services: WPS002, WPS008, INF051, OTH001, SME005

Standard service support levels:

Service Availability: 99.5%¹

Standardised time to deliver new service instance: 1 working day (if all service prerequisites are met).

¹ The availability of the Service is calculated by the following formula:
(Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes.

Service Restoration: Full priority resolution times and generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency SLA, SSP or any other agreement with the Customers.

Service Reporting:

The reports included in the service are:

- Impact on service availability and service performance reports at Service Access Point (SAP) (via incidents);
- Incident management report base on ITSM tickets and trend analysis;
- Change management and ASI report based on ITSM tickets.

Quarterly Reports:

- Quantity of NDW001 instantiated at each Command and geographical location;
- Number of service requests per feature.

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Service Cost / Price:

The unit of measure for the service is per user and includes mandatory security software (if applicable), licenses and subscriptions.

The number of Service Units will be determined based on active user accounts on the respective CIS where the NDW001 NATO Digital Workplace Service is utilized. The annual service rate includes the in-service support rate for the service.

Service initiation cost:

New service instances are requested by submitting a Customer Request Form (CRF)¹.

For customers who are procuring new quantities of the service, a service initiation rate (procurement and deployment of the service components) shall apply as a one-time cost.

The annual service rate includes the in-service support rate for the service.

Compatible NDW003 Devices

Same NDW001 user can select one or more of the following devices:

Service Type	Remarks
NDW003-A Static Desktop (Workstation) Device	Static Desktop Devices are no longer used at Low Side (NU level) unless required to support specific customer requirements or for security reasons. For standard Low Side usage, please see NDW003-C Portable (Laptop) Device service type.
NDW003-B Thin Client Device	Requires supporting Virtual Desktop Infrastructure (VDI) backend to be present
NDW003-C Portable (Laptop) Device	Laptops, though with different specifications, will be captured under this single flavour in 2026 CCSC. Tablets running Microsoft Windows Operating system will be considered under NDW003-C service type.
NDW003-E Smartphone/Tablet (iOS device only)	Provides phone/tablet (hardware); additionally customers should procure WPS016-B/1/2/3/4/5 or WPS016-D SecuSUITE as required for their mobility requirements.
NDW003-F Monitors	Covers all monitor types and screen sizes available in the NCI Agency's procurement catalogue. The default monitor size is 24 inch.
NDW003-G KVM (Keyboard/Video/Mouse) Switch	The service covers the variety of KVM switches with required number of inputs/outputs. The default model supports two monitor outputs and two device inputs.

NDW002 NATO Digital Workplace Service (High Side)

Service ID: NDW002

Service Name: NATO Digital Workplace Service (High Side)

Portfolio Group: NATO Digital Workplace Services

Service/Product Status: Available

Service Description: The NATO Digital Workplace Service is the work environment for NATO staff. NDW002 has all the features and functionalities required in NATO's Digital Workplace, so Staff can connect, communicate and collaborate in an effective way taking Staff Productivity and Enablement to the next level.

Value Proposition: NDW002 provides comprehensive and mutually complementary set of features and functionalities as one cohesive intelligence to the NATO Enterprise. Unified set of features and functionalities will enable Staff to easily connect, communicate and collaborate within and across Entities.

NDW002 not only simplifies the standard service offerings but also unites the NATO Enterprise by ensuring that previously fragmented features and functionality are available to all NATO Enterprise Staff.

The availability of a NATO Digital Workplace with common set of features and functionalities allows digital business process transformation, end-user Digital Enablement (adoption, digital dexterity 1& satisfaction) and drives further the NATO Digital Transformation.

Service Features: The Service provides the following features and functionalities:

- Computing Platform (Operating System) depending on the selected hardware (NDW003);
- Operating system and baseline application management (patching, upgrades, etc.);
- Mandatory Security Components;
- Digital #OneNATO name (ENTITY | LASTNAME Firstname | *Optional Fields*);
- Unified NATO identity (@ENTITY.nato.int or @nato.int) with one personal mailbox;
- Digital Signature (hardware authentication token)²;
- Personal Storage Space (Microsoft OneDrive, 20GB per user);
- Collaboration (Skype for Business for instant messaging, email, Polycom for NCS users);
- Content Creation (Microsoft Office Suite, Adobe Acrobat Reader);
- Access to digital enablement content (training material, videos, etc.);
- Packaging of the mandatory software present on every devices (Enterprise Candidate Applications);
- Distribution to end users, support for installation of software applications procured through APP001 service and/or available on A2SL (software license costs are not included and has to be requested via APP001 service separately).

¹ Digital Dexterity is the beliefs, the mindsets and behaviors, that accelerated digital business transformation (Harvard Business Review 2021)

² The feature will be available after the implementation of NS PKI. The authorised token is a smartcard.

Service Ordering and Request: The new service instances are requested by submitting a Customer Request Form (CRF) After a service is initiated, the in-service support phase for the service is managed through annual Service Agreements with each customer. The service fee for this service is charged to each Agency customer directly, meaning the service charges are not covered by the NATO central funding channels for NATO, therefore each customer requests/orders this service directly themselves.

For IT Incidents, Request for Information (RFI) and Service Requests (SR) regarding this service, the Enterprise Service Operations Centre (ESOC) is the NCI Agency's Single Point of Contact (SPOC) for all eligible Customers and Users.

Service Flavours: NATO Digital Workplace Service (High Side) flavours:

NDW002 comes only in one service flavour, which is covering the high side (NS). The equivalent service for lower content classification can be found under NDW001 NATO Digital Workplace Service (Low Side).

Available Networks:

The Service is available on NATO Secret NCIA-managed CIS.

Service pre-requisites:

NDW003 Personal Workspace - Managed Device Service (a maximum number of devices as covered via WPS003 Enterprise User License Service);
WPS003 Enterprise User License Service.
SEC015 Security Certificate Service (for digital signature)

Underlying Services: WPS002, WPS008, APP064, OTH001

Standard service support levels:

Service Availability: 99.5%

The availability of the Service is calculated by the following formula:

$(\text{Available Minutes}^* - \text{Downtime}) / \text{Available Minutes} \times 100$

*Minutes available during agreed reporting period excluding planned maintenance minutes.

Standardised time to deliver new service instance: 1 working day (if all service prerequisites are met).

Service Restoration: Where the service is unavailable, the service restoration period follows the ABIPAT and Service Level Agreements in force. Additional support can be requested through a Customer Request Form (CRF).

Service Reporting:

The reports included in the service are:

- Impact on service availability and service performance reports at Service Access Point (SAP) (via incidents);
- Incident management report base on ITSM tickets and trend analysis;

- Change management and ASI report based on ITSM tickets.

Quarterly Reports:

- Quantity of NDW002 instantiated at each Command and geographical location;
- Number of service requests per feature.

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG

Support Hours:

- Centralized Service Desk agents are available Mon-Thurs 06.00-22.00 CET, Fri 06.00-20.00 CET. Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.
- Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time at Service Access Point). Outside of these hours, On-Call personnel is available to intervene within 1h.

Service Cost / Price:

The unit of measure for the service is per user and includes mandatory security software and licenses (if applicable) and subscriptions.

The number of Service Units will be determined based on active user accounts on the respective CIS where the NDW002 NATO Digital Workplace Service is utilized.

Service initiation cost:

New service instances are requested by submitting a Customer Request Form (CRF).

For customers who are procuring new quantities of the service, a service initiation rate (procurement and deployment of the service components) shall apply as a one-time cost.

The annual service rate includes the in-service support rate for the service.

Compatible NDW003 Devices

Same NDW002 user can select one or more of the following devices:

Service Type	Remarks
NDW003-A Static Desktop (Workstation) Device	

NDW003-B Thin Client Device	Requires supporting Virtual Desktop Infrastructure (VDI) backend to be present
NDW003-F Monitors	Covers all monitor types and screen sizes available in the NCI Agency's procurement catalogue. The default monitor size is 24 inch.
NDW003-G KVM (Keyboard/Video/Mouse) Switch	The default model supports two monitor outputs and two device inputs.

NDW003 Personal Workspace – Managed Device Service

Service ID: NDW003

Service Name: Personal Workspace - Managed Device Service

Portfolio Group: NATO Digital Workplace Services

Service/Product Status: Available

Service Description: The Personal Workspace - Managed Device Service provides users with various personal computing devices, accessories and peripherals that allows them to utilize the NDW001/NDW002 NATO Digital Workplace Services or other Application Services which require a physical device in order to secure a connection to NATO networks (in a specific security domain).

The Personal Workspace - Managed Device Service includes commodity devices such as workstations, laptops, thin clients, smartphone/tablets, respective peripherals and accessories required to create an effective digital workplace. The service includes the minimum required operating system or specific firmware necessary to achieve the stated service quality. Additionally, the service includes mandatory security tools, accessories, licenses and subscriptions required to maintain the service quality of the device.

The service includes Company Owned NATO Operated (CONO) devices and the associated full lifecycle management.

Value Proposition: The service offers a managed device enabling users to perform their duties in an effective and consistent way. It is closely linked to the NDW001/NDW002 NATO Digital Workplace Services, which provides the comprehensive Digital Workplace experience at both Low Side (NU level) and High Side (NS level), ensuring operational efficiency and effectiveness throughout the NATO Enterprise.

The Personal Workspace - Managed Device Service provides active obsolescence management, i.e. the replacement of the devices at the end of their lifecycle is included in the service rate. Replacement procedure will be initiated by NCIA.

Service Features: The features varies per type, please see the section “Service Flavours” for detailed information on the feature of each type

Service Flavours: The Personal Workspace - Managed Device Service flavours are:

NDW003-A Static Desktop (Workstation) Device - This device is a workstation that needs to be connected to a wired network. It features a keyboard and mouse. In exceptional cases, a Static Desktop Device may be provided as a standalone device. Monitors are *not* included in the service type and needs to be selected in the quantities required through the NDW003-F service. A total of three monitors can be connected by default.

Note: Static Desktop Devices are no longer used at Low Side (NU level) unless required to support specific customer requirements or for security reasons. For

standard Low Side usage, please see NDW003-C Portable (Laptop) Device service type.

NDW003-B Thin Client Device - This device is a computing device that runs from resources stored on a central server instead of a local hard drive, commonly referenced to as a Virtual Desktop Infrastructure (VDI) device. Thin clients work by connecting remotely to a server-based computing environment where most applications, sensitive data and memory are stored with the need to be connected to a wired network. It features a keyboard and mouse. Monitors are *not* included in the service type and needs to be selected in the quantities required through the NDW003-F service.

NDW003-C Portable (Laptop) Device - This device can either operate as stand-alone device, be connected to a wired network or connected to a wireless network. It comes with an external power adaptor, keyboard, mouse, docking station, headset, bag by default. All other accessories are be ordered separately.

Note: The NDW003-C Portable (Laptop) Device, can be connected to NCI Agency supported CIS through various connectivity:

- Static connection, i.e. cabled connection to an existing low-side or high-side network (high-side requires Wifi and cellular connectivity disabled)
- Remotely through either WiFi or cellular connectivity (low-side only).

Note: Tablets running Microsoft Windows Operating system will be considered under NDW003-C service type.

NDW003-E Smartphone/Tablet (iOS device only) - this service flavour accounts for an Apple iPhone/iPad device including its associated management configuration ensuring the device is in compliance with applicable cyber security configuration (Mobile Device Management (MDM) configuration). It comes by default with an external power adaptor, protective cover and screen protector. Tablets will have a protective cover with embedded keyboard by default. Additional accessories like authorized Bluetooth headset (Apple AirPods) and Apple Pencil can be ordered at extra cost and are not covered by lifecycle management.

NDW003-F Monitors - This service type covers all types of monitors (display systems) that are connected to other NDW003 service types. The service type covers all screen sizes available in the NCI Agency's procurement catalogue¹. The default monitor size is 24 inch.

NDW003-G KVM (Keyboard/Video/Mouse) Switch – This service provides a KVM switch used to connect securely personal computing devices from various classifications to the same monitor, keyboard and mouse. The service covers the variety of KVM switches with required number of inputs/outputs. The default model supports two monitor outputs and two device inputs.

¹ Until NCI Agency's procurement catalogue is ready all customer requests for a new specific monitors and large screen displays will be coordinated and processed through the CRF process.

The following accessories are included as standard with each service flavour:

Service Type	Service Unit	Standard accessories included	Remarks
NDW003-A	Per Device	Keyboard and mouse	
NDW003-B	Per Device	Keyboard and mouse	
NDW003-C	Per Device	Keyboard, mouse, docking station, headset, bag	Accessories to be refined in the future by using different sets depending on end-user "personas"
NDW003-E	Per Device	Smartphone: Power adaptor, protective cover and screen protector. Tablets: Power adaptor, protective cover with embedded keyboard	Additional accessories, like Bluetooth headsets to be ordered separately
NDW003-F	Per Device	÷	
NDW003-G	Per Device	÷	

Available Networks:

The Service flavours are available at different classification levels as per the following table (÷ meaning not available, ✓ meaning available) :

Service Type	Stand Alone Device	NATO Unclassified	NATO Restricted	NATO Secret*/ Mission Secret**	Lifecycle (years)
NDW003-A	÷ See note 3	÷ See note 1	÷ See note 1	✓	5
NDW003-B See note 2	÷	✓	✓	✓	6
NDW003-C	✓ See note 3	✓	÷ See note 4	÷	3
NDW003-E	÷	✓	✓	÷	3
NDW003-F	✓	✓	✓	✓	5

NDW003-G	÷	✓	✓	✓	5

*** TEMPEST testing of devices used on High Side (NS/MS) is mandatory**

****Devices can be purchased to operate on MS network but network itself is not managed by NDW001 or NDW002**

Note 1: Supported if required by specific performance based applications or to meet specific customer's needs.

Note 2: Requires supporting Virtual Desktop Infrastructure (VDI) backend to be present.

Note 3: Stand Alone Devices intelligence is managed and supported through WPS002-1, it is also the Customer's responsibility to ensure that the devices are operated according to NATO policies.

Note 4: Current NR Laptops are still covered under WPS006.

Please note: For devices used on the high-side (NS/MS), TEMPEST testing of each devices is mandatory. The cost for TEMPEST testing is a one-time only cost which will be included in the Service Initiation cost.

Service pre-requisites:

INF001 LAN Service (not applicable to standalone devices)

Underlying Services: OTH001, SME005

Standard service support levels:

Service Availability: 99.59%

The availability of the Service is calculated by the following formula:

$(\text{Available Minutes}^* - \text{Downtime}) / \text{Available Minutes} \times 100$

*Minutes available during agreed reporting period excluding planned maintenance minutes.

Standardised time to deliver new service instance: 3 working day (including delivery, configuration and installation to the end-user if all service prerequisites are met).

Service Restoration: Where the service is unavailable, the service restoration period follows the ABIPAT and Service Level Agreements or other agreements in force. Additional support can be requested through a Customer Request Form (CRF).

Service Reporting:

The reports included in the service are:

- Impact on service availability and service performance reports at Service Access Point (SAP) (via incidents);
- Incident management report base on ITSM tickets and trend analysis;
- Change management and ASI report based on ITSM tickets.

Quarterly Reports:

Based on final outsourced contract but expected to include:

- Quantity of NDW003 instantiated at each Command and geographical location;
- Service flavour lifetime against life expectancy;
- Number of faulty Service flavours replaced;
- Number of service requests;
- Recommended number of assets per service type eligible for life-cycle replacement within next 12-18 months (only until life-cycle replacement is included in service rates)
- Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

Service Cost / Price:

The unit of measure for the service is per device and includes mandatory security software and licenses (if applicable) and subscriptions plus standard accessories described in each service flavour.

The new service instances are requested by submitting a Customer Request Form (CRF). For customers who are requesting new quantities of the service, a service initiation cost (procurement and deployment of the service components) shall apply as a one-time cost, to be communicated to the customers via Price Proposal following a CRF submission.

The annual service rate for the service includes the annual in-service-support costs for the service and lifecycle replacement cost share of the assets.

Annex – Each NDW003 service flavour is mapped to the eligible intelligence services (NDW001 or NDW002) which can utilise the device type per network classification. Same NDW001 user can use multiple eligible NDW003 devices; similarly same NDW002 user can use multiple eligible NDW003 devices (up to the maximum number of devices as covered via WPS003 Enterprise User License Service flavour selected)

Service Type	Stand Alone Device	NATO Unclassified	NATO Secret/Mission Secret
NDW003-A	Intelligence supported through WPS002-1	NDW001 See note 1 above	NDW002
NDW003-B	Intelligence supported through WPS002-1	NDW001	NDW002
NDW003-C	Intelligence supported through WPS002-1	NDW001	
NDW003-E	Intelligence not supported	NDW001	
NDW003-F	Intelligence not supported	NDW001	NDW002
NDW003-G	Intelligence not supported	NDW001	NDW002

NDW005 Digital Events Service

Service ID: NDW005

Service Name: Digital Events Service

Portfolio Group: NATO Digital Workplace Services

Service/Product Status: Available

Service Description: The NATO Digital Workplace (NDW) Digital Events Service provides an enterprise-level solution for managing and executing digital and hybrid events. Designed to eliminate technical and logistical challenges for the customer, the service offers structured event coordination, audience engagement, and high-quality execution.

Value Proposition: The service enables customers to conduct professional, high-impact events with minimal operational burden. By providing access to enterprise-level event management, audience engagement tools, and expert technical support, the service allows event organizers to focus on content while ensuring seamless execution. Through a combination of digital platform integration, real-time moderation, and full A/V production capabilities, the service enhances accessibility and engagement across NATO's digital landscape.

Service Flavours: The NDW Digital Events Service is divided into multiple event types, each offering varying levels of support. Customers can select the appropriate service(s) based on their requirements, ensuring tailored event execution.

- NDW005-A provides access to a NATO-accredited virtual event platform along with professional event management and coordination, while customers remain responsible for their own audio-video (A/V) streaming.
- NDW005-B is a comprehensive, full-service solution that includes NATO-managed streaming, professional-grade studio equipment, and full production support at the NU level.
- NDW005-C is for customers requiring professional-grade A/V support for live-streaming. It can be purchased as a standalone service, or in combination with NDW005-A to ensure a fully supported livestream.
- NDW005-D provides the option to add additional event days and extended A/V support, ensuring a **modular and scalable approach** to digital event management.
- NDW005-E provides secure, NATO-accredited digital event platform while managing their own audio-video (A/V) streaming set-up (direct A/V feed from NR REACH, or A/V feed managed by external providers).

NDW005-A Standard Digital/Hybrid Event (Customer-Managed Streaming): Designed for customers who require access to a secure, NATO-accredited digital event platform while managing their own audio-video (A/V) streaming set-up (direct A/V feed from NU or public device, or A/V feed managed by external providers). This option supports both meetings and events up to four (4) hours long on Webex Meetings and Webex Webinars, providing flexibility for different event types. NDW event coordinators provide virtual assistance in event planning, participant management, and moderation to ensure seamless execution.

Customers requiring a full-day of event must purchase two quantities of NDW005-A. To purchase professional-grade equipment and A/V support to capture the livestream for an NDW005-A event, please see service flavour NDW005-C.

Service Features

- Up to 4 hours of live event
- Event platform (Webex Meeting or Webex Webinar)
- Personalized event link and relevant joining details
- Studio integration (studio or video stream provided by customer)
- Online event rehearsals (up to 1)
- Q&A, Polling, Chat capabilities
- Breakout rooms
- Simple registration page capability
- Real-time moderation (support with Q&A, Polling Chat, Lobby Management)
- Option for online integration of simultaneous interpretation audio feeds (interpreter must be provided by customer)
- Provision of event recording (up to 1 hour post-production)
- Post-event performance analytics

NDW005-B Advanced Digital Event for NU (NDW-Managed Streaming): NDW005-B is a full-package digital event experience, combining the most advanced event platform with full-service NATO-managed streaming and production support. This option is ideal for large-scale, high-visibility events that require flawless execution, immersive audience engagement, and professional-grade video and audio quality.

This service includes the use of Webex (Socio) Events, an advanced event management platform that provides enhanced attendee interaction capabilities, real-time networking tools, and seamless hybrid event integration. Attendees benefit from a fully customized event hub, while organizers have access to a robust back-end system for streamlined registration, engagement tracking, and post-event analytics.

In addition to platform access, NDW005-B includes NATO-managed livestreaming and full production support. A dedicated, on-site technical team ensures the highest level of video and audio quality, using professional-grade cameras, lighting, and mixing equipment. The service covers everything from pre-event rehearsals and technical setup to real-time monitoring and live moderation, ensuring a polished and professional delivery.

This package is the optimal choice for NATO multi-day conferences and highly publicized digital events where production quality and seamless execution are critical.

Service Features

- Up to 8 hours of live event support
- Travel within Europe
- Event platform for customized, branded registration page (Webex (Socio) Events)
- Conference Livestream Hub (Webex (Socio) Events)
- Conference hub mobile application (Webex (Socio) Events)
- Studio integration (studio or A/V stream provided by NDW)
- Contact management: email templates, attendee communications
- Event rehearsals (up to 2)
- Live engagement tools: Online networking, chat, video rooms, polling, live word-mapping, Q&A, question up-voting
- Option for online integration of simultaneous interpretation audio feeds (interpreter must be provided by customer)
- Live online moderation support, provided on-site
- Event recording and up to 4 hours of post-production
- Post-event performance analytics and dedicated lessons-learned presentation
- + Professional-grade studio livestreaming

NDW005-C Professional A/V Support for Livestreaming: Intended for customers who require dedicated professional audio-video (A/V) support for streaming or recording their events. Technical audio-video support can be provided at the NU, NR, and NS levels. It can be purchased alongside NDW005-A to fulfil requirements for a fully supported event production, or as a standalone service for events requiring only technical support in audio-video production or high-quality recording.

Service Features

- Up to 4 hours of live event support
- Travel within Europe
- Add onto NDW005-A, or purchase independently.
- Customized technical set-up for streaming or recording events at any content classification (NU, NR, NS) (online collaboration platform must pre-arranged by customer or purchased through NDW005-A)
- On-site technical support including room preparation, rehearsals, delivery of event, breakdown of equipment.
- Provision of event recording (up to 3 hours post-production)

NDW005-D Additional Day of Event Support: Provides customers the option to add additional days of support to their event, enabling continuous coordination, registration management, and technical execution. Customers may purchase one (1) quantity of this service flavour in addition to NDW005-B or NDW005-C for each additional day of event support required.

Service Features

- On-site technical support and coordination for an extended event duration
- Continued registration management, audience engagement, and event moderation
- Customized technical adjustments for evolving event requirements
- Travel within Europe

NDW005-E Standard Digital/Hybrid Event on NR Reach (Customer-Managed Streaming): Designed for NCIA personnel who require access to a secure, NATO-accredited digital event platform while managing their own audio-video (A/V) streaming set-up (direct A/V feed from NR Reach, or A/V feed managed by external providers). This option supports both meetings and events up to four (4) hours long on Skype Large Conference. NDW event coordinators assist in event planning, participant engagement, and real-time moderation to ensure a seamless execution.

Customers requiring a full-day of event support event must purchase two quantities of NDW005-E. To purchase professional-grade equipment and A/V support to capture the livestream for an NDW005-E event, please see service flavour NDW005-C.

Service Features

- Up to 4 hours of live event support
- Event platform (Skype Large Conference)
- Personalized event link
- Q&A, Polling, Chat capabilities
- Studio integration (studio or livestream provided by customer)
- Online event rehearsals (up to 1)
- Real-time moderation (online support with Q&A, Polling Chat, Lobby Management)
- Post-event performance analytics
- Max # participants 700

Available Networks:

The Service flavours are available at different classification levels as per the following table:

Service Type	NATO Unclassified	NATO Restricted	NATO Secret
NDW005-A	✓	÷	÷
NDW005-B	✓	÷	÷

NDW005-C	✓	✓	✓
NDW005-D	✓	✓	✓
NDW005-E	÷	✓	÷

Service Cost/Price

Pricing is based on event complexity and support level. Each service flavour is a separate purchase, ensuring customers can tailor their event package according to their needs.

NDW006 Information and Knowledge Management Applications

Service ID: NDW006

Service Name: Information and Knowledge Management Applications

Portfolio Group: NATO Digital Workplace Application Service

Services Service/Product Status: Available

Service Description: The NATO Digital Workplace (NDW) Information and Knowledge Management Applications service provides a suite of five components:

- Tasker Tracker Application Service (TT+)
 - Provides information management capabilities for the tracking of organizational tasking activities and for the tracking of all Allied Operations and Missions (AOM) related project information
- Project Implementation Tasker Tracker Application Service (PITT)
 - Provides the capability to track all Allied Operations and Missions (AOM) related project information, facilitates collaborative work, and establishes a coherency to the CUR (Crisis Response Operations Urgent Requirements) management of all projects through a centralized approach, which support management boards and additional supporting services, such as search and a report centre
- Enterprise Document Management Application Service (EDMS)
 - Provides collaborative information management capability for Document and Records Management, with functionalities for standardised document creation, management, storage and retrieval
- Business Process Management (BPM) tool
 - Provides a software tool that automates recurring processes. The tool can be used to automate a wide range of tasks, from simple leave requests to complex business processes. It can also be used to improve the efficiency of business by helping staff to document, identify and optimize the business processes.
- NATO Information Portal Application Service (NIP)
 - Provides a secure, online collaborative environment for users to create, capture, store, manage, broadcast, publish, view, and search all types of digital content. It allows organizational elements to establish an Intranet rich collaboration environment by utilising and combining web information publishing and portal feature options.

Value Proposition: The NDW Information and Knowledge Management (IKM) Applications service provides a set of collaborative, efficient, and auditable applications for managing organizational information and tasks, improving situational awareness and

business operations. It offers easy access to documents with granular access control, streamlined location and retrieval, and secure storage, all while complying with NATO standards and IKM policies. Furthermore, it empowers users to collaborate effectively by sharing information, co-creating documentation, and publishing content directly, enabling effective IKM within a controlled and protected information lifecycle. Finally, by facilitating BPM, the service helps organizations automate and optimize their processes, leading to increased efficiency, process excellence, and continuous improvement.

Service Features:

Tasker Tracker Plus (TT+) and Project Implementation Tasker Tracker (PITT): Provide the following core functionalities:

- Multi- user collaborative tasking
- Advanced Task Search Engine
- Sub-Tasking (including favourites)
- Reporting on Taskers by Office and Status
- Business Intelligence
- Traffic Light Monitoring System
- Integrated Document Management.

Enterprise Document Management Application Service (EDMS): Provides the following core functionalities:

- Customizable organisational and data structures
- “Private” and “Public” document libraries
- Versioning
- Check in/check out functionality
- Search and browsing of documents
- Record Centre Workflow and Drop-Off library
- Alerting capability
- Access control
- Creation of documents by templates
- Document conversion into PDF files
- Distribution and archiving of documents, compatible with the NATO Archive
- Physical Media Management
- Integration with (optional) Tasker Tracker Plus (TT+) and NATO Information Portal (NIP).

Business Process Management (BPM): Provides the following core functionalities:

- Easy to use using a drag and drop interface, no coding required.
- Usable for a wide range of processes, from simple to complex.
- Scalable: can handle any number of users and processes.
- Integrates with the other IKM tools and connects to external systems.
- Improves process visibility: helps users understand their own processes better.
- Reduces errors eliminating human error by automating tasks.
- Saves time and improves productivity automating repetitive tasks, freeing up staff for more important work.

NATO Information Portal (NIP): Provides the following core functionalities:

- Dashboard: a standard landing page for each Command.
- Command Structure: implementation of the Command Structure to navigate the NIP and reorganization driven by metadata.
- Dedicated Command Page, with Alert State and Footer links categorized by groups.
- Site Templates: Landing page, Document Collaboration, Exercise, etc.
- Events Management: approval workflow for publishing on Command page, events sharing across Commands and Departments, conference room management, bookings & attendees management with notifications and calendar functionalities using Exchange, registration lists to events.
- Articles Management: Command page publishing approval workflow, articles sharing across Commands and Departments.
- Data and Information Management: Countries, Key Individuals and Organizations, Exercises & Operations, Training.
- Enforced Classification of Information: Highest classification displayed on each page according to the information item highest classification.
- Search Centre: Search using refiners supporting information discovery.
- Bi-Strategic Commands IKM Change Management Board (BICMB): change request management tool driving the continuous improvement of the IKM Tools.
- Integration (optional) with EDMS: documents displayed on Command Page, Departments, Nations and Community.
- Integration (optional) with TT+: Taskers displayed on Command page from Command TT+, Taskers assigned to their respective office displayed on their respective Department/COI pages.

Service Flavours: The NDW IKM Applications service is available in two flavours:

NDW006-A IKM Profile

- Tasker Tracker Applications Service (TT+)
- Project Tracker Applications Service (PITT)
- Enterprise Document Management Application Service (EDMS)
- Business Process Management (BPM)

NDW006-B NIP Profile

- NATO Information Portal (NIP)

Available Networks:

The Service flavours are available at different classification levels as per the following table:

Service Type	Public	NATO Unclassified	NATO Restricted	NATO Secret	Mission Secret	NATO Partner Network (For NNHQ)
NDW006-A	✓	✓	✓	✓	✓	✓
NDW006-B	✓	✓	✓	✓	✓	✓

NDW001 NATO Digital Workplace Service (Low Side) or NDW002 NATO Digital Workplace Service (High Side)

WPS003 Enterprise User License Service

For services hosted on NATO Infrastructure

- PLT003 Web Hosting Service
- PLT006 Database Platform Services

For services hosted on NPCL (NATO Public Cloud)

- PLT010 Cloud Services Management and Integration Services

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration Priority: P2.

The Standard Service support comprises the following activities:

- **Operation:** Application monitoring, log management, batch jobs management, backup & restore, auditing, Service Requests fulfilment.
- **Corrective Maintenance:** Diagnosis and removal of the causes and the effects of any malfunction affecting the Service.
- **Preventive Maintenance:** Preventive actions needed to avoid future malfunctions.
- **Adaptive Maintenance:** Adjustment of the Service in order to adapt to the minor changes of sub-system components (i.e. Operating System, Database Management System, Browser, SharePoint and SharePoint add-ons). Major changes of sub-system components can be requested submitting a Customer Request Form (CRF).

- **Minor Perfective Maintenance:** Development of up to one minor change¹ per month².

Available NCI Academy Training not covered by service cost:

A2536	Tasker Tracker + (TT+)
A2539	TT+ - Functional Administrator
A2537	EDMS - Enterprise Document Management System User
A2538	EDMS - Functional Administrator

Service Cost / Price: The unit of measure for the service is “per user”. Since the service is designed for the general use by all the users of each customer, the number of user will be assumed to be equal to the sum of the “NATO Peacetime Establishment (PE)” users plus the “NATO Non-Peacetime Establishment (NPE)” users. The cost of the service does not include the cost of all the underlying service prerequisites. Each instance of the service is counted separately (so for example, if the same user is using two different instances of the service on two different networks, the user is counted twice).

The total amount of the service delivery price is calculated in accordance with specifically arranged conditions of the service delivery. Specifically, service rates are dependant from the underlying platform being hosted either by NATO assets on premises or by commercial service providers for the NATO unclassified contents.

¹ A “minor change” is defined as a limited enhancement of an existing functionality or the creation of a new functionality of the Service that requires in total not more than five (5) person days in order to be designed, developed and tested. All the enhancement requests are screened, vetted and prioritized by the “Bi-SC IKM Change Management Board” before being developed.

² This activity will be paused during major implementation projects affecting the Service.

NDW007 NATO AI Chatbot

Service ID: NDW007

Service Name: NATO AI Chatbot

Portfolio Group: NATO Digital Workplace Application Service

Service/Product Status: Available

Service Description: The NATO Digital Workplace (NDW) NATO AI Chatbot service is an advanced Artificial Intelligence (AI)-powered virtual assistant designed to support NATO personnel in their daily tasks. It leverages Large Language Models (LLMs), currently Open AI ChatGPT, to deliver informative and timely responses to your questions, enhancing productivity and efficiency.

It is accessible exclusively from NATO end-user devices ensuring the confidentiality and integrity of all inputs and outputs.

The service is currently available up to NATO Unclassified.

Value Proposition: The NDW NATO AI Chatbot service provides the following key benefits:

- **Faster Information Retrieval:** Provides instant answers to customer queries, accelerating decision-making and improving efficiency.
- **Enhanced Text Processing:** Helps customers with tasks like document generation, summarization, and translation.
- **Improved Information Accuracy:** Accesses curated databases and NATO-specific knowledge to ensure customers receive accurate and relevant information.
- **Increased Security:** All interactions occur through NATO's secure network, safeguarding the confidentiality and integrity of customer information.

By using the chatbot on NATO devices, customers can achieve their goals faster and more effectively, contributing to the overall success of NATO's operations.

Service Features:

- **NATO Knowledge Base:** The chatbot is equipped with NATO-specific information on operations, policies, and procedures (pending NOS approval) to provide tailored and accurate responses.
- **Secure Interface:** Access the chatbot through NATO's secure network, ensuring all data exchanges comply with NATO's cybersecurity protocols.
- **Multilingual Support:** The chatbot can understand and respond in multiple languages.
- **High Availability:** The service provides 24/7 access to information and chatbot functionalities.
- **User-Friendly Interface:** The chatbot's intuitive interface requires minimal training, making it accessible to all NATO personnel regardless of technical expertise.



- **Document Upload:** The chatbot allows uploading documents up to NU (pending NOS approval) and ask questions on it as well as requesting unofficial translations, summaries, etc.

Available Networks:

NATO Unclassified

Standard service support levels:

Service Availability: 99%

Service Restoration Priority: P2

Service Cost/Price: The unit of measure for the service is “per user”. Since the service is designed for the general use by all the users of each customer, the number of user will be assumed to be equal to the sum of the “NATO Peacetime Establishment (PE)” users plus the “NATO Non-Peacetime Establishment (NPE)” users.



Workplace Services



WPS001 Managed Device Services

Service transitioned to NDW001, NDW002,NDW003.

WPS002 Enterprise Identity Access Management Service

Service ID: WPS002

Service Name: Enterprise Identity Access Management Service

Portfolio Group: Workplace Services

Service Description: The Enterprise Identity Access Management Service (E-IDAM) provides identities (including provisioning and de-provisioning of User Accounts, Privileged Accounts, Service Accounts, Computer Accounts), and the capability to share trusted identity information between different domains and to Enterprise users. The information on identities retrieved from different authoritative sources. Additionally, the service includes the provisioning of personal storage space (minimum 20 GB) for storing personal information and documents (only for WPS002-1A: User Account on-premises)¹.

The Service allows controlled access based services. The access services can be available across domains utilising AD-Federation. It offers a Single Sign On experience for users with a valid NATO Enterprise Identity. The service also provides Directory Synchronization enabling Global Address List synchronisation to the NCI Agency External Customers, Mission environments, and Allied Nations.

The Service provisions, operates, maintains, retires authentication subsystems like LDAP, Domain Controllers, Active Directory, ADFS, MIM, SSO. The service can delegate limited authority to the supporting elements.

Value proposition: E-IDAM provides value to customers through the hosting and sharing of identity information across multiple identity stores, improving data quality and reducing the administrative burden for connected systems. This ensures a coherent set of identity data from authoritative sources, while increasing the security posture of the NATO Enterprise.

The Service provides access to the Alliance GAL, including structured contact information. It enables searching for people and groups somewhere in the Alliance.

The Service allows the users to securely access different NATO networks, and it enables the NCI Agency to manage and maintain the access to the identities to track and control usage of resources ensuring only authorized users are accessing relevant services/resources.

Furthermore, it enables enhanced security, prevention of oversubscription to the services.

The Service provides access to the Alliance GAL, including structured contact information. It enables searching for people and groups somewhere in the Alliance.

The Service allows the users to securely access different NATO networks, and it enables the NCI Agency to manage and maintain the access to the identities to track and control usage of resources ensuring only authorized users are accessing relevant services/resources. Furthermore, it enables enhanced security, prevention of oversubscription to the services.

¹ NCIA is assessing this statement as it is not aligned with the current capability of the underlying central storage service and might be subject to modification in the following catalogue releases.

Service Features:

Identity Management shared information across multiple identity stores, improving data quality and reducing overhead for connected systems. Identity information can be synchronised between different affiliates, supported by automated workflows and enables account provisioning and de-provisioning. Data sources/consumers can use native interface of E-IDAM to retrieve or modify it through industry standard protocols and mechanism (like LDAPs). Moreover, Lifecycle management (from provisioning to de-provisioning) of Identity and its attributes is being provided with E-IDAM.

Access Management is available for the compatible services requiring authentication for users and/or resources. The access management (authentication/control/validation) is provided by credential management, security group memberships, and policies (like GPO), also through integration with NATO PKI.

Account Lifecycle Management provisioned and managed on-premises and off-premises (cloud) by WPS002 including the secure and sanitized environment. The accounts on the cloud requires additional licenses to reach and consume cloud resources, as well as security & safety requirements dedicated to the cloud provider, also it brings efficiency with automation by nature of cloud.

Web Federation provides cross-domain authentication to reach web-based resources seamlessly (SSO) to increase the user experience and to enable the secure service on Windows based ADFS.

DNS Federation - distribution of domain name system (DNS) authority across multiple, independent entities or organizations (i.e. nations, partners) to enhance resiliency, scalability and diversity within the DNS ecosystem, reducing the risk of single points of failure and promoting decentralization.

Data Directory Synchronization (DDS) is provided through a number of directory synchronisation servers, which are inter-connected to identity directories of the participating NATO organisations and Nations. The DDS allows the exchange of shared identity information (such as Display Name, Organisation Name, E-Mail Addresses and other relevant contact information) between service subscribers. GAL Sync is a flavour of the Data Directory Synchronization.

Service Flavours: The Service is available in multiple flavours, with the following options:

WPS002-1 User Account¹ (On-premises or Off-premises): Per account

WPS002-2 Web Federation: Per connection.

¹ The WPS002-1 User Account service flavour is delivered as underlying service of NDW001 - NATO Digital Workplace Service (Low Side) or NDW002 - NATO Digital Workplace Service (High Side). For specific cases where the Customer requires a user without a full work environment (as depicted in the Service Description of NDW001 and NDW002 services), the flavour can be Purchased separately.

WPS002-3 Data Directory Synchronization: Per connection.

WPS002-4 DNS Federation: Per connection

Available on:

NATO Unclassified
 NATO Restricted
 NATO Secret
 Mission Secret
 NATO Partner network
 Public Cloud (limited with Security conditions)

Service Prerequisites:

INF002 NATO Network Point of Presence
 INF003 Enterprise Internet Access Service
 INF004 Infrastructure Hosting Service
 INF005 Infrastructure Integration Service
 INF016 Infrastructure Back-up and Archiving Service
 PLT006 Database Platform Service
 SEC011 Gateway Security Service

Underlying Services: OTH001

Standard Service support levels:

Service Availability¹ Target:

For service flavour "Account LM":	99.0%
For service flavour "Federation":	99.9% during Support Hours 99.5% outside of Support Hours
For service flavour "DDS":	99.0%

Standardised time to deliver new service instance: 1 working days² (creation of new account)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) Restoration Time is 2 (two) working days with 80% INC IN SLA Enterprise-wide

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated based on the followings:

- "Available Minutes": during agreed reporting period excluding planned maintenance minutes

$$\text{(Available Minutes - Downtime)} / \text{Available Minutes} \times 100$$

² Taking into consideration that all required documentation is provided to ESOC

N.B. Service will be restored under the condition that underlying services are available. Priority Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA

Service Reporting: Service Reports will be based on the number of incidents (solved/failed), Service Request. Also availability figures will be populated from the service monitoring toolsets/features.

Available NCI Academy Training not covered by service cost: No training is available on the Agency's catalogue yet. There will not be any training for the end users since this is an enabling service.

Service Cost / Price: The unit of measure for the service varies depending on the flavours.

WPS002-1 User Account: Per User Account

WPS002-2 Web Federation: Per connection.

WPS002-3 Data Directory Synchronization: Per connection.

WPS002-4 DNS Federation: Per connection.

Please see Service Rates document for standard rates applicable to the service.

WPS003 Enterprise User License Service

Service ID: WPS003

Service Name: Enterprise User License Service

Portfolio Group: NATO Digital Workplace Services

Service Description: The Enterprise User License Service provides a Microsoft Enterprise User License based on NATO User Profile which comes in two pre-packaged profiles (NATO Standard and NATO Delegation User) of which all two contain the same licensing components and the same functionality to the user, however with different number of qualified devices that the licenses are allowed to run on.

Value proposition: This service allows users to access via multiple devices (desktop, laptop, thin clients...), on multiple networks (business, operational, missions & exercises), and also to leverage the mobile devices that are increasingly typifying our environment (phones, tablets, iOS, Android). This user approach achieves both of the aims of reduced cost, and simplified licensing and management.

Service Features: The key licensing components cover the core business needs of the users for Windows, Office and server access across the NATO Enterprise. The licensing components included are:

- Windows: Windows Software Assurance per user provides access to Windows Enterprise for install or VDI across devices
- MS Office: On-premise version of MS Office Professional Plus Suite across Windows devices
- Enterprise Client Access: enterprise client access licenses to access the server functionality in Windows, Exchange, SharePoint per user across devices
- SQL Client Access: Client access to SQL Server per user across devices
- Skype for Business Plus Client Access: Client access to enterprise-grade instant messaging and phone features in Skype for Business per user.

Service Flavours: The Enterprise User License Service is available in the following flavours:

- **WPS003-1 NATO Standard Profile** authorizes use of the licensed Products on **up to 5 (five)** Qualified Devices on each network.
- **WPS003-3 NATO Delegation User** authorizes the use of the Product on a **single** Qualified Device by **up to 8 (eight) users** where the Software is installed (i.e. delegations, NMRs, third party).

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret



Service prerequisites:

None

Underlying Services: OTH001, SME005

Standard Service support levels: N/A

Service Cost / Price: The unit of measure for the Service is Per User or Per Device, depending on the flavour. Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate.

Please see Service Rates document for standard rates applicable to the service.

WPS006 REACH Mobile Workplace Service

Service ID: WPS006

Service Name: REACH Mobile Workplace Service

Portfolio Group: NATO Digital Workplace Services

Service Description: The REACH Mobile workplace Service provides client devices (Laptops) that allow to connect to the NATO Restricted network.

Additionally, the Service includes:

- A User Account, Password and PKI token to access the NR.AIS Network (WPS002);
- A mailbox on the Restricted network (WPS012); and
- An IM Collaboration Account (WPS012).

The Laptop Client device is loaded with the office automation software (MS Office Professional Suite), Windows operating system, VPN client software, and security and management tools.

Value proposition: The REACH Mobile workplace service is a bundle of four customer-facing services (Managed Device Service, Enterprise Identity Access Management Service, E-mail Service, IM collaboration Service), infrastructure and platform services, offered as a single service package for the NATO Restricted Network.

Service Features: Same as the four individual services comprised in this service offer. There is an additional option for a Static work position which consists of a docking station, dual LCD Monitor, VTC camera, Keyboard and mouse. (This option is only applicable for the Portable Client Device service flavour).

Service Flavours:

Portable Client Device (Laptop) – provides a Laptop device that needs to be connected to a wired or wireless network. The laptop comes with a power supply, a carrying case, a headset, and an external mouse.

Optional Static Work position – only applicable for a portable client device service flavour; provides a docking station for the portable device, dual LCD monitors, a VTC camera, a keyboard, and a mouse.

Available on:

NATO Restricted

Service Prerequisites:

WPS003 Enterprise User License Service

WPS008 ESOC Service – mandatory service for each WPS006 device.

Underlying Services: APP064, WPS008

Standard Service support levels:

Service Availability Target : 99.0%

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Service Cost / Price: Unit of measure used for service quantification is Per Device.

Please see Service Delivery Lifecycle Stages section for the lifecycle stages of a service along with the corresponding deliverables and the service rates applicable in each stage.

Please see Service Rates document for standard rates applicable to the service.

WPS007 Print/ Scan/ Copy Service

Service ID: WPS007

Service Name: Print/Scan/Copy Service

Portfolio Group: NATO Digital Workplace Services

Service Description: The Print/Scan/Copy Service includes the management of multifunctional devices (MFDs), i.e. devices with combined print, scan and copy functionality, as well as document management and workflow solutions to improve an organization's printing environment. The Print/Scan/Copy service enables the user to create hardcopies of digital content or to digitise hardcopies.

Under this service, NCI Agency uses a large framework contract with a global supplier of multifunctional devices to ensure standardization, and service reliability across the Alliance at the most efficient price.

These multifunctional devices are by default enabled with badge-controlled authentication and can be acquired in various TEMPEST tested variants.

Depending on the service flavour selected, lifecycle replacement after five (5) years is included at no additional cost to the customer¹.

Value proposition: The Print/Scan/Copy Service supports various Business Processes across the Enterprise by performing multiple office imaging tasks, such as input, output and transmission of documents. It allows electronic content to be re-produced in hardcopy for easy reading, commenting, obtaining physical signatures, etc. The service also allows physical paper content to be electronically stored and transmitted to relevant recipients on NCI Agency supported system.

Service Types: The Print/Scan/Copy service includes four service flavours²:

WPS007-1-A (Large Print Volume - A3 MFD 5XXX Series)

This printer comes with the following technical specifications:

- 40 ppm
- Optimum print volume: 5.000 – 30.000 per month
- Lifetime 2.000.000 prints
- Color & B&W Printing/Scanning/Copying
- Double-sided Printing/Scanning/Copying
- Document Feeder for scanning of multiple documents
- Scan directly to users' email address
- Multiple paper sizes possible: A3-A4-A5-A6-Envelopes
- User Identification through RFID card

¹ One-time cost related to TEMPEST testing is not including in the five (5) year service rate.

² Exact MFD device models can change without prior notification due to contractual changes and/or end of service notifications from current supplier.

WPS007-1-B (A3 MFD 3XXX Series)

This printer comes with the following technical specifications:

- 30 ppm
- Optimum print volume: 5.000 – 10.000 per month
- Lifetime 1.000.000 prints
- Color & B&W Printing/Scanning/Copying
- Double-sided Printing/Scanning/Copying
- Document Feeder for scanning of multiple documents
- Scan directly to users' email address
- Multiple paper sizes possible: A3-A4-A5-A6-Envelopes
- User Identification through RFID card

WPS007-1-C (A4 MFD)

This printer comes with the following technical specifications:

- 35ppm
- Color & B&W Printing/Scanning/Copying
- Double-sided Printing/Scanning/Copying
- Document Feeder for scanning of multiple documents
- Scan directly to users' email address
- Multiple paper sizes possible: A4-A5-A6-Envelopes
- User Identification through RFID card

WPS007-1-D (A4 Desktop-sized MFD)¹

This printer comes with the following technical specifications:

- 33ppm
- Color & B&W Printing/Scanning/Copying
- Double-sided Printing/Scanning/Copying
- Document Feeder for scanning of multiple documents
- Scan directly to users' email address
- Multiple paper sizes possible: A4-A5-A6-Envelopes
- User Identification through RFID card

WPS007-1-E: Plotter (Large Format Printer) and Large Reprographic Printers

Due to the limited quantities of plotters within NATO, and their specific usage, this service flavour is not available as part of the large framework contract. The service is offered with a Service Initiation cost and annual service rate calculated upon request.

¹ For optimal performance and reliability, it is recommended that desktop printers be connected directly via USB and not through the network.

Compatible Accessories

Printers can be equipped with various accessories, per flavour. These need to be selected up front at service initiation stage and cannot be deselected throughout the duration of the service commitment.

WPS007-1-A Compatible Accessories

WPS007-1-A1 Stapler finisher
WPS007-1-A2 Booklet finisher
WPS007-1-A3 High capacity paper feeder
WPS007-1-A4 Hole puncher

WPS007-1-B Compatible Accessories

WPS007-1-B1 Stapler finisher
WPS007-1-B2 Booklet finisher
WPS007-1-B3 High capacity paper feeder
WPS007-1-B4 Hole puncher

WPS007-1-C Compatible Accessories

WPS007-1-C3 High capacity paper feeder

For MFDs used on high side (NS/MS), any optional features need to be requested at the service initiation stage, and it is not possible to have optional features retrofitted due to the mandatory requirement for TEMPEST testing of the MFDs.

Accessories are not possible for WPS007-1-D or WPS007-1-E.

Standard Service Features: The Print/Scan/Copy Service provides the following minimum features:

- Grey-scale and Colour printing
- Single and Double-sided printing (paper size varies according to service flavour selected)
- Document feeder for scanning of multiple documents
- Scan directly to user's email address
- Paper Input Trays supporting multiple paper sizes
- Copy functionality, single and duplex sided
- Toner and toner electronic advanced notification for replacement
- User authentication through scanning of RFID card (typically AMIS badge)

Available on:

NCI Agency supported CIS on both low side (NU/NR) and high-side (NS/MS).

Note: For MFDs used on the high-side (NS/MS), TEMPEST testing of each MFDs is mandatory. The cost for TEMPEST testing is a one-time only cost which will be included in the Service Initiation cost. The Annual Service rate for both TEMPEST and non-TEMPEST tested printers remains the same. The standard delivery time is 14 weeks (including TEMPEST).

Service prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) or NDW002 NATO Digital Workplace Service (High Side) (for scanning functionality only)

NDW003 Personal Workspace - Managed Device Service (or qualified connected device)

Standard Service Support Levels:

General service availability* target is 99.0% with Priority Resolution Times and Generic Service Priority Assignment Matrix in accordance with the NCI Agency standardised Service Level Agreements in force.

Only if one of the following incident conditions are met incident will be considered as wide spread outage and will be assigned with the agreed incident restoration priority:

- Service is unavailable to all users in an organisation. For example users are unable to select the print queue while attempting to print, or the entire print capability is unavailable.
- 50% or more of the MFDs deployed in a single geographical location are unavailable.

ACO/ACT Customers: Incident prioritisation and service restoration requirements are in accordance with the Aligned Baseline Incident Priority Assignment Table (ABIPAT) agreed in the SLAs. Service Request / Request Fulfilment prioritisation and service installation requirements are in accordance with implementation time targets agreed in SLAs.

Service Cost/Price:

The unit of measure, used for service costing is per Multi-Functional Device¹ and per type of printed page.

¹ For new entities, not already consuming the WPS007 Print/Copy/Scan Service, there is a one-time cost of EUR7,200. This covers the instantiation of the backend required plus socialization efforts enabling an effective use of the service

The exact service rate is not yet calculated, but is estimated due to ongoing renewal of the active contract with current supplier. For 2024 budgetary purposes the following annual service rates are recommended to be used***:

*** The service rate is based on a full five-year service commitment. In case of shorter service commitment, the investment cost of the MFDs will be borne at service instantiation.

The annual service rate will equally be lower depending on the length of the service commitment decided. Exact service rate calculation will be provided at price proposal stage.

Please see Service Rates document for standard rates applicable to the service.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

Additional service reporting requirements can be requested through the respective SLAs it may be subject to additional service fees

WPS009 Unclassified Voice Collaboration Service

Service ID: WPS009

Service Name: Unclassified Voice Collaboration Service

Portfolio Group: NATO Digital Workplace Services

Service Description: The Voice Collaboration Service provides the ability to collaborate and communicate through audio with the telephony subscribers on NATO and National military unclassified networks, as well as commercial fixed and mobile telephony networks.

Value proposition: The Service allows voice communication between two or more parties from any location. This increases flexibility and saves cost, as no travel is required.

Service Features: The different device modalities (analogue phone, Voice over IP phone, Software Client, etc.) as well as service features are highly dependent of the specific location where the service is provided. Same applies for the various features and functions such as conferencing capabilities, hunt groups, voice mail, pickup-groups, call forwarding, etc.

With each instance of the service, either a static desk phone or a Software Client will be provided with an assigned telephone number, consisting of an internal 4-digit extension and a location-based prefix.

With the assigned telephone number, the user can place and receive calls to/from NDN, NCN and commercial networks. To be able to call from softphone a local national breakout connection to commercial networks is required

Service covers in-service support of end-to-end telephony services including the replacement of hardware and software in case of an incident. Default calling permissions (flat-rate contract) includes calls to all NATO subscribers, National Military networks and Europe (including US, Canada, Türkiye) telephony networks. Other calling permissions can be provided but they are subject to customized configuration.

The procurement of software and hardware (including end-user devices) and lifecycle replacement is excluded from the service support cost (O&M) and must be procured separately.

Service Ordering and Request: The new service instances are requested by submitting a Customer Request Form (CRF).

After a service is initiated, the in-service support phase for the service is managed through annual Service Agreements with each customer.

The service fee for this service is charged to each Agency customer directly, meaning the service charges are not covered by the NATO central funding channels for NATO, therefore each customer requests/orders this service directly themselves.

For IT Incidents, Request for Information (RFI) and Service Requests (SR) regarding this service, the Operations Centre is the NCI Agency's Single Point of Contact (SPOC) for all eligible Customers and Users.

Service Flavours:

Available flavours are the following:

WPS009-1 - Voice Collaboration (Calling) Service: Provided as a telephone number and assigned to a Desk Phone or a Softphone (via Skype for business). The user can place and receive calls from/to the assigned telephone number.

WPS009- 2 -Business-to-Business Federation (B2B)¹: Provides NATO users the possibility to communicate through audio with external Voice networks such as Nations, Missions, Deployed CIS, NGO's.

Available on:

Static Desk Phone: NATO Voice Network. Highest content classification: UNCLASSIFIED

Softphone (Skype for Business): Available on NU and REACH networks. Highest content classification: UNCLASSIFIED

Service prerequisites:

INF001 LAN Service

WPS012 Workstream Collaboration Service (for Softphone only)

Underlying Services: OTH001, TRA002

Standard Service support levels:

Service Availability² Target: 99.5%

Standardised time to deliver new service instance³: 3 working days (installation and configuration of new phone device)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Higher service availability and restoration targets can be negotiated and funded through the respective SLAs.

ACO/ACT Customers: Incident prioritisation and service restoration requirements are in accordance with the Aligned Baseline Incident Priority Assignment Table (ABIPAT)

¹ B2B is not applicable to common-funded Customers

² The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

³ Provided the underlying infrastructure is ready and devices are on site

agreed in the SLAs. Service Request / Request Fulfilment prioritisation and service installation requirements are in accordance with implementation time targets agreed in SLAs.

Other Customers. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency SLAs and SSPs with respective customers.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

Phone billing service for the period (optional, upon request)

Asset and Configuration Management report

Additional service reporting requirements can be requested through the respective SLAs it may be subject to additional service fees.

Available NCI Academy Training not covered by service cost:

A0095	NATO Voice over IP Foundation
A0097	NATO Call Manager & Voice over Secure IP (VoSIP)
A0101	NATO C4ISR Orientation for Officers and NCO's
A0932	DCIS CES Voice Technician

Please note that this training is not funded through the service rate and it is added in the catalogue to familiarize the service users community with the available courses as part of the agency academy courses offerings.

Service Cost / Price:

The unit of measure for the Voice Collaboration (Calling) Service is per the telephone number assigned. The unit for the Business-to-Business Federation (B2B) service is per instance implemented.

Please see Service Rates document for standard rates applicable to the service.

WPS010 Video (VTC) Collaboration Service

Service ID: WPS010

Service Name: Video (VTC) Collaboration Service

Portfolio Group: NATO Digital Workplace Services

Service Description: The Video (VTC) Collaboration Service provides users the ability to collaborate and communicate through video and audio. It allows users from different geographical location to have face-to-face like collaboration as well as it supports multi-user, multi-location collaboration.

Value Proposition: The Service allows individuals and groups to interact easily, which enables a more flexible and efficient exercise of the Command and Control with significant savings in travel time and cost.

Service Features: The Service features include scheduling, VIP monitoring, conferencing, recording, playback and streaming, and connectivity of third parties.

Service Flavours:

WPS010-1 VTC Soft Client: provides users with an application (Polycom RealPresence Desktop) installed on the managed/qualified device. The flavour requires a camera and a microphone (in-built or as addition).

This is a best-effort service and HD quality is not guaranteed due to infrastructure limitations. Please also note that the infrastructure has a limitation for 500 concurrent calls.

WPS010-2 VTC System Only: consists of a VTC CODEC, which is integrated in a non-NATO Studio Wide VTC Room (a conference room with audio/video assets which belong to the local site and is therefore not part of the VTC Service).

WPS010-3 Desktop Dedicated Terminal: provides users with a dedicated VTC terminal (Polycom) connected to the network, which can be either:

- Desktop VTC Terminal, or
- Huddle/small room based system.

Conference room VTC: integrates with Conference room setups that become VTC enabled – it's provided with a camera and microphone and can be integrated with Conference room projection and presentation devices. The flavour has a range of room systems depending on their size, number supported participants, and the need for mobility, as follows:

- Roll About VTC system:
 - **WPS010-4 VTC Room - Roll About SDS (Single Domain);**
 - **WPS010-5 VTC Room - Roll About DDS (Dual Domain);**
- **WPS010-6 15-man room VTC system (dual domain system);**

- **WPS010-7 25-man room VTC system (dual domain system);**
- **WPS010-8 50-man room VTC system (dual domain system);**
- **WPS010-9 175-man room VTC system (dual domain system).**

WPS010-10 Immersive Telepresence Meeting (ITP) Room VTC : This service flavour uses enhanced conference room technologies and provides the illusion of an in person meeting through the use of multiple screens in an 'across the table' setup. Available only as single domain system.

WPS010-11 VTC B2B (Business to Business) Connection: provides a possibility to communicate through audio and video between NATO users and external VTC networks such as Nations, Missions, Deployed CIS, NGO's and GO's.

Available on:

NATO Unclassified (including public access)
NATO Restricted
NATO Secret
NATO Partner Network (For NNHQ)

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side).

Underlying Services: OTH001, TRA002

Standard Service Support Levels:

Service Availability Target: 99.0% (exception: Soft Client flavour)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0244	NATO HD VTC Facilitator

Please note that this training is not funded through the service rate and it is added in the catalogue to familiarize the service users community with the available courses as part of the agency academy courses offerings.

Service Cost / Price: The unit of measure for the Service is Per Client Device, except for the VTC B2B flavour, where the unit of measure is Per VTC B2B Package. A VTC B2B Package includes up to 300 calls per year, limited to up to 5 simultaneous calls.

Please see Service Delivery Lifecycle Stages section for the lifecycle stages of a service along with the corresponding deliverables and the service rates applicable in each stage.

Please see Service Rates document for standard rates applicable to the service.

In special cases there are discounts offered:

	Case	Discount
1	The customer has its own local support contract for equipment maintenance	10%
2	The customer provides the L1 support	20%
3	Combination of 1 and 2	30%

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

Asset and Configuration Management report

Additional service reporting requirements can be requested through the respective SLAs it may be subject to additional service fees.

WPS011 IP Television (IPTV) Service

Service ID: WPS011

Service Name: IP Television (IPTV)

Portfolio Group: NATO Digital Workplace Services

Service Description: IP Television Service provides the user with commercial cable television service as well as NATO specific channels. This service provides numerous channels, primarily focused on news and informational events, and offered in a variety of languages used in NATO.

Value Proposition: The IP Television Service offers the user an ability to leverage a fully managed and operated contractor service inside the New NATO Headquarters. This allows the user to keep up to date with news events. In addition to commercial news, the user can also view NATO channels which provide NATO news as well as can provide streamed videos of HQ briefings. This aids operational efficiency and effectiveness and supports situational awareness throughout the headquarters.

Service Features: The IP Television Service includes a fully managed and operated commercial capability augmented with NATO information. IP Television can be a full service providing the television, trolley and channels or as small as offering the channels and a connection SetTopBox (STB).

Business users can access three of the main news channels on their NATO managed mobile device.

Nations and staff can request additional channels that offer specific programming or national specific content. These channels can be ordered separately and the price is based on the requested licensing.

Service Flavours:

IP Television – This service supports the office environment. The 55” television is mounted on a trolley and connected to the floor box plug in a specific office or meeting room

Soft client – This service flavour allows the users to access the IPTV channels from their devices, provided through the managed device services.

Available on:

IPTV Flavour – Public networkSoft client flavour – NATO Restricted and NATO Unclassified

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side).

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Device.

Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate.

Please see Service Rates document for standard rates applicable to the service.

#	Channel Name	#	Channel Name
1	La Une	23	CNBC-E
2	La deux	24	Sky news
3	La trois	25	Channel 5
4	France24	26	ITV 1
5	TV5Monde	27	ITV 2
6	BBC World	28	ITV 4
7	MTV	29	BBC News
8	CNN	30	ITV 3
9	Euronews	31	RTP-International
10	Nederland 1	32	RAI News24
11	Nederland 2	33	TVR International
12	Nederland 3	34	ARD
13	BBC1	35	TV-8
14	BBC2	36	ATV
15	National Geographic Channel HD	37	TRT 1
16	RAI 1	38	TRT 2 (Haber)
17	RAI 2	39	TRT Turk
18	RAI 3	40	CNN Turk
19	Animal Planet	41	Haber Turk
20	Aljazeera	42	TGRT
21	Discovery Channel	43	TA3
22	Eurosport	44	PRO TV International

WPS012 Workstream Collaboration Service

Service ID: WPS012

Service Name: Workstream Collaboration Service

Portfolio Group: NATO Digital Workplace Services

Service Description: The Workstream Collaboration Service provides a persistent, shared conversational workspace for shared mailboxes (e.g. for groups, functional, common or otherwise shared).

Value Proposition: The service supports both ad-hoc collaboration (informal e-mail).

Service Features: WPS012 (Workstream Collaboration Service) covers the informal shared email aspects of collaboration within the future NATO Digital Workplace.

Standard Microsoft Exchange Mailbox is accessible through a thick mail client (MS Outlook) or through the web-based client (OWA). The standard mailbox size is 10GB. Mailboxes are available to support group mailboxes, functional mailboxes or shared mailboxes only.

For personal mailboxes, customers should refer to NDW001 NATO Digital Workplace Service (Low Side) or NDW002 NATO Digital Workplace Service (High Side).

For the more formal, i.e. consultation, aspects of collaboration please refer to WPS010 (Video (VTC) Collaboration Service).

Service Ordering and Request: The new service instances are requested and created by submitting standardised service request (work order) through the ITSM toolset; for customers there is no specific service initiation cost associated with Workstream Collaboration Service.¹

After a service is initiated, the in-service support phase for the service is managed through annual Service Agreements with each customer.

The service fee for this service is charged to each Agency customer directly, meaning the service charges are not covered by the NATO central funding channels for NATO, therefore each customer requests/orders this service directly themselves.

For IT Incidents, Request for Information (RFI) and Service Requests (SR) regarding this service, the Operations Centre is the NCI Agency's Single Point of Contact (SPOC) for all eligible Customers and Users.

Service Flavours: The service is available in two flavours

- **WPS012-A:** Provides a shared mailbox (group, functional, common, etc).
- **WPS012-EF (External Federation):** Enables an external entity to federate with NATO e-mail or Skype for Business services on the available networks the service is provisioned at. It contains only the fees to configure and bring the service alive in terms of human resource and Microsoft consultancy. It does not include any hardware or

¹ Non-common funded customers via a Customer Request Form (CRF).

license fees required by the federating entity. The service is per capability, either e-mail or Skype for Business. When both capabilities are federated, the fee is two times the service cost.

Available on*:

NATO Unclassified

NATO Restricted

NATO Secret

Mission Secret

Other specialized NATO networks (e.g. NATO Partner network and alike)

*Note: The features and functionality available in each network can deviate due to security constraints and local security policies as determined by the relevant Security Accreditation Authority (SAA). Equally, the products used to provide the service can be different depending on the classification of the network in use.

Service Prerequisites:

NDW003 Managed Device Service (connected or standalone flavours)

Standard Service Support Levels:

Service Availability Target: 99.0%

Standardised time to deliver service: 1 working day (creation of new shared/functional/group e-mail account)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full priority resolution times and generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Impact on service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

CIS Security and Cyber report

Asset and Configuration Management report

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

Service Cost / Price: The unit of measure for the Service is "per instance". Each instance of the Service will be counted separately (i.e. if the same shared mailbox is used on two different networks, it will be counted twice).

All exceptions to the service instance calculation method will be agreed between the Provider and the Customer and documented in the individual SLAs/SSPs accordingly.

For WPS012-EF flavour the unit of measure is per connection. Skype federation is counted as one connection and e-mail federation is counted as an extra connection. If external customers require both federations, the quantity shall be two connections.

WPS014 Secure Voice Service

Service ID: WPS014

Service Name: Secure Voice Service

Portfolio Group: NATO Digital Workplace Services

Service Description: The Secure Voice Service is a voice collaboration service that provides user with the ability to collaborate and communicate through audio and audio/video in a secure network environment. Depending on the selected service flavour, this Service enables communication within or to other Voice Secure Domains outside of NATO VoSIP network (e.g. BICES).

Value Proposition: The Service enables real-time secure communication between more parties. This dramatically increases the effectiveness of the Command and Control and provides additional flexibility and efficiency to it, by saving time and cos of usually required travel.

By providing service flavours for the secure voice telephone number (WPS014-1) separate from the physical Voice over Secure IP (VoSIP) device, customers have the flexibility to purchase their required amount of telephone numbers without having to purchase the matching number of devices. This allows for device sharing (e.g. in common areas).

WPS014-5 also includes active obsolescence and are provided using a device-as-a-service model. The cost of replacement of the devices at the end of their lifecycle is therefore included in the service rate.

Service Features: Secure Calls, Secure Video Calls, Secure Conferencing Calls, Secure Video Conferencing Calls, Hunt Groups, Pick Up Groups, Call Forwarding, and Extension Mobility Service are provided on the available NATO security domain

Service Flavours:

WPS014-1 Secure Voice Service – Telephone Number: Provides a secure voice telephone number assigned.

WPS014-2 Secure Mobile phone (SECTRA)¹: Provides a mobile ability to collaborate and communicate through audio in a closed NATO only SECTRA secure network environment. The device allows voice connections up to SECRET level and SMS up to RESTRICTED level within the NATO SECTRA environment.

WPS014-4 Business to Business Federation (B2B): Provides NATO users the possibility to communicate through audio and video with external Voice networks such as Nations, Missions, Deployed CIS, NGOs and GOs.

¹ Hardware Connector to a Secure Mobile Phone Flavour (Tiger/S 7401 docking station connector) – can be provided when needed as part of the service rate without O&M extra charges, commands can buy the cable/connector through the CRF process

WPS014-5 Secure Voice Service – Desk Phone: Provides a physical Voice over Secure IP (VoSIP) device used on High Side (NS/MS). The device comes with mandatory cyber security components and required software/licenses. This flavour covers both voice-only or voice/video devices.

Available on:

NATO Secret

Mission Secret

Service Prerequisites:

INF001 LAN Service

SEC011 Gateway Security Service (To Secure Domains outside NATO VoSIP Network) whenever needed.

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0095	NATO Voice over IP Foundation
A0097	NATO Call Manager & Voice over Secure IP (VoSIP)

Service Cost / Price:

The unit of measure for WPS014-1 is Per User.

The unit of measure for WPS014-2 and WPS014-5 is Per Device.

The unit of measure for WPS014-4 Voice Business to Business (B2B) is per B2B connection.

Please see Service Rates document for standard rates applicable to the service.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Service availability and service performance reports at Service Access Point (SAP) (via incidents).

Incident management report base on ITSM tickets and trend analysis.

Change management and ASI report based on ITSM tickets.

Asset and Configuration Management report.

Additional service reporting requirements can be requested through the respective SLAs it may be subject to additional service fees.

WPS015 Voice Loop Service

Service ID: WPS015

Service Name: Voice Loop Service

Portfolio Group: NATO Digital Workplace Services

Service Description: The Voice Loop Service provides the user with the ability to communicate with a group of users through audio.

Value Proposition: Voice Loop Service allows easy communication between more than one party (CAOC's and CRC's). This increases reliability, flexibility and response time to Static Air Defence Centre mission of Air and Controlling Policing over NATO North and South Region.

Service Features: The Service allows the user to participate in different Conferences (Voice Loops) established with different locations with the ability of IP Voice recording.

Voice Loop Conferences: Voice Loop provides the user the ability to participate in a permanent open conference with all the participants in a specific region.

Voice Recording: Allows IP Voice capture and preservation system, therefore constant recording of all Voice Loop voice content

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

For IP Phone: INF001 LAN Service

For Networking: INF005 Infrastructure Integration Service

For Communication: INF014 Transmission Service

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0095	NATO Voice over IP Foundation
A0097	NATO Call Manager & Voice over Secure IP (VoSIP)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

WPS016 Enterprise Managed Mobility Service

Service ID: WPS016

Service Name: Enterprise Managed Mobility Service

Portfolio Group: NATO Digital Workplace Services

Service/Product Status: Available

Service Description: The Enterprise Managed Mobility Service provides the users with various flavour of mobile communication solutions ranging from a basic cellular subscription to fully managed communication solutions enabling users to communicate up to NATO Restricted level.

Value Proposition: The Service offers additional subscription-based services to eligible users¹.

Service Features:

- Mobile subscription, cellular provider expense management, and data cost management;
- Mobile Secure Communication on smartphones, enabling users to communicate up to NATO Restricted level.

Service/Product Request: New service instances are requested by submitting a Customer Request Form (CRF). For customers who are procuring new quantities of the service, the service initiation rate (procurement and deployment of the service components) shall apply as a one-time cost.

Service Flavours:

WPS016-B1 Cellular Subscription (Profile Plan 1 - Basic) (*note)

Unlimited SMS/Calls in EU+ (if user is based in the EU+ only)

Unlimited SMS/Calls in USA (if user is based in the USA only)

WPS016-B2 Cellular Subscription (Profile Plan 2 - Standard) (*note)

Unlimited SMS/Calls in EU+ (if user is based in the EU+ only)

10GB internet in EU+ (if user is based in the EU+ only)

Unlimited SMS/Calls in USA (if the User is based in the USA only)

10GB internet in USA (if the User is based in the USA only)

WPS016-B3 Cellular Subscription (Profile Plan 3 - Traveller) (*note)

¹ Eligible users are users with an existing NDW003-E Smartphone/Tablet (iOS device only) device and the corresponding NDW001 NATO Digital Workplace Service (Low Side) services

Unlimited SMS/Calls in EU+ (if user is based in the EU+ only)
 10GB internet in EU+ (if user is based in the EU+ only)
 Unlimited SMS/Calls in USA (if the User is based in the USA only)
 10GB internet in USA (if the User is based in the USA only)
 3GB in Extended Roaming Countries*

WPS016-B4 Cellular Subscription (Profile Plan 4 - Traveller Unlimited) (*note)

Unlimited SMS/Calls in EU+ (if user is based in the EU+ only)
 Unlimited Data in EU+ (if the User is based in EU+ only)
 Unlimited SMS/Calls in USA (if the User is based in the USA only)
 Unlimited internet in USA (if the User is based in the USA only)
 5GB in Extended Roaming Countries

WPS016-B5 Cellular Subscription (Profile Plan 5 - Data Plan), single device use (*note)

Unlimited GB Data in EU+ (if the User is based in EU+ only)
 Unlimited GB Data in USA (if the User is based in the USA only)

WPS016-B6 Mobile Hotspot Wi-Fi (MIFI), multiple device use (*note)

A MiFi device is a small router or hotspot that typically works over a cellular connection, using network data to create a Wi-Fi connection for laptops, tablets, and other devices. The WPS016-B6 Flavour only covers the mobile subscription for the device. Device itself is subject to specific initiation costs.

Unlimited GB Data in EU+ (if the User is based in EU+ only)
 Unlimited GB Data in USA (if the User is based in the USA only)

WPS016-D Mobile Secure Communication on smartphones - SecuSUITE

Provides secure voice and chat solution on managed smartphones, up to NATO secuRestricted level by using authorized commercial solution.

*note: The subscription cost is location/country specific and only indicated as an average for SLA/SSP planning purpose. For unlimited subscriptions, commercial fair-use restrictions may apply

Note 1: Due to supply chain security and other important security considerations, any smartphone and/or tablet connecting to a NCI Agency supported CIS shall have both the actual device (NDW003-E) and its cellular subscription, i.e. SIM Cards (WPS016-Bx), provided by the NCI Agency.

Note 2: Tablets provided through NDW003-E can have an optional SIM card slot installed which can be used for gaining access to the Internet. If the SIM card slot is utilized in tablets that connects remotely to a NCI Agency supported CIS, the cellular subscription must be provided via WPS016-B5 service flavour.

Provision of cellular subscriptions for legacy devices or Phones not provided by the NCI Agency is optional through WPS016-B1 or WPS016-B2 service flavour only.

Note 3: Customers who selects only the NDW003-E service flavour, i.e. the device only without a cellular subscription, will have the device considered as a standalone SIM-less device. Customers will be able to use their own cellular subscriptions while still having a supported smartphone/device.

If a customer wants to utilize their own cellular subscription together with the NDW001 NATO Digital Workplace Service (Low Side) service flavour, the NCI Agency will need to review the contractual and legal agreements of the customer's cellular subscription. This is mandatory to ensure the required contractual and legal frameworks are in place for secure and reliable connectivity to a NCI Agency supported CIS. The cost for the review will be charged to the customer on a cost reimbursable basis.

Available Networks:

Standalone (see note 3 above)

NCI Agency supported CIS on low side (NU/NR)

Service pre-requisites:

NDW003-E Smartphone/Tablet (iOS device only)

NDW001 NATO Digital Workplace Service (Low Side)

Service Cost / Price:

The unit of measure for the service is per subscription.

Service ID	Service Name	Service Flavour/Option	Service Unit
WPS016	Enterprise Managed Mobility Service	WPS016-B1: Cellular Subscription (Profile Plan 1 - Basic)	Per SIM Card
		WPS016-B2: Cellular Subscription (Profile Plan 2 - Standard)	Per SIM Card
		WPS016-B3: Cellular Subscription (Profile Plan 3 - Traveller)	Per SIM Card
		WPS016-B4: Cellular Subscription (Profile Plan 4 - Traveller Unlimited)	Per SIM Card
		WPS016-B5: Cellular Subscription (Profile Plan 5 - Data Plan Hotspot)	Per SIM Card
		WPS016-B6: WPS016-B6 Mobile Hotspot Wi-Fi (MIFI)	Per Sim Card
		WPS016-D: Mobile Secure Communication on smartphones - SecuSUITE	Per subscription



This page is left blank intentionally



Infrastructure Services

INF001 Local Area Network (LAN) Service

Service ID: INF001

Service Name: LAN Service

Portfolio Group: Infrastructure Service

Service Description: The LAN service provides users with local network connectivity. The LAN service is crucial to enable collaboration and communication. The LAN service is provided as a cabled infrastructure for all networks and as a wireless infrastructure for accessing only the unclassified and restricted networks.

Value Proposition: The LAN Service is a vital component enabling all local users to connect to the wider network. It is the key enabler for accessing all NATO customer facing services such as Voice and Video, as well as Internet, and enabling services such as security and management. The Service allows all entitled users to access shared NATO services and data across the NATO Enterprise.

Wi-Fi connections provide additional flexibility, allowing users to connect to the network from anywhere within the relevant Wi-Fi footprint, preventing users from being 'tied' to their desks.

Service Features: LAN Service is available on the NATO Security domains in wired and, in selected locations, as Wireless (Wi-Fi) configurations. The LAN Service will be capacity sized to support the number of connected devices and Users. This is with the understanding that all equipment is located within the same building and that the cabling system is available. The service does not cover the cabling through the building walls, as this is considered part of the building infrastructure.

Service Flavours: The LAN Service is available in the following flavours:

Wired – This service flavour provides a physical connection to terminate and connect devices to one of the NATO networks.

By utilising NCIA deployed LAN Service, users are able to operate on all wired NATO networks including, but not limited to:

- NATO Unclassified
- NATO Restricted
- NATO Secret
- Mission Secret (when invoked)

Wireless - This service flavour provides the ability to connect a specific client device to a network wirelessly by providing access to centrally managed end-User devices via Enterprise and Mobility SSIDs (Service Set Identifier). Service does not cover the Guest WiFi and Scientific WiFi, which are out of scope).

By utilising NCIA deployed LAN Service, users are able to operate on all wireless NATO networks including:

- NATO Unclassified

NATO Restricted

Available on:

NATO Unclassified
NATO Restricted
NATO Secret – only wired
Mission Secret (when invoked) – only wired

Service Prerequisites:

INF002 NGCS PoP Service

Underlying Services: INF046, INF051, OTH001

Standard Service Support Levels:

		Availability Target	Service Period	Restoration
During hours	Support	99.9 %	1 hour	
Outside hours	Support	99.5 %	4 hours	

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

While this provides a standard availability target for the service, regional support arrangements and therefore the availability targets may vary and should be agreed during the SLA discussions.

Service Cost / Price: The unit of measure for the Service is Per Port, with 24 ports being the minimum orderable quantity. The number of ports required for a customer is in accordance with the quantity of devices requested through NDW003-A Static Desktop (Workstation) Device, NDW003-B Thin Client Device, NDW003-C Portable(Laptop) Device, NDW003-E Smartphone/Tablet(iOS device only) and WPS006-1 Reach Mobile Workplace Service Basic multiplied by 2.

Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate. Please see Service Rates document for standard rates applicable to the service.

INF002 NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service

Service ID: INF002

Service Name: NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service

Portfolio Group: Infrastructure Services

Service Description: The NGCS PoP Service primarily provides the infrastructure at points between communicating entities, where a connection is required. The NATO Network POP Service is defined as the provision of the infrastructure assets, capacity provisioning, and cyber security management elements that enable the user to establish any-to-any connectivity at supported sites and between connected networks. It has a dependency on INF014, which provides the connection between sites. At each security domain classification, this service is a direct enabler of other customer facing services like: INF001, INF035, as well as 3rd party customers serviced via Point to Point EVCs or PCN type interfaces.

Value Proposition: The Service is an integral component in enabling users to connect and collaborate between each other in support of the majority of NATO business activities and processes.

Service Features: The Service is available across all NATO Security Domains. It features the WAN Infrastructure Assets (Protected Core Access equipment in line with the valid Technical Architecture) and Cyber Security Management (layered security present at connectivity access points).

NGCS Service Flavours: The exact specification of each service flavour may vary subject to equipment and suppliers but can be described as follows:

- **INF002P - Pico PoP:** this flavour provides the termination of medium bandwidth transmission services with links up to 100 Mbit/s. Pico PoP flavour supports user communities up to 100 users. PicoPoPs are generally customer (SSP) funded and include a Customer Edge Device (CED) e.g. NFIUs. They also provide dedicated or shared services to support NNCCRS.
- **INF002L - Legacy PoP (Remote extension):** this flavour provides the termination of small bandwidth transmission services (less than 100Mbit/s links). Remote extension services are also required to support up to 100 users. Considered as a legacy connection for existing services that do not meet the NGCS target architecture requirements; it is no longer offered as a new service. It does not include a NED or CED. This service flavour is marked to be discontinued, with service delivery being migrated to the INF002 – NNG service flavour, in line with AFS concepts.

NGCS Service Flavour Enhancements: NGCS PoPs may be extended or enhanced with the following:

- **INF002NNG - NATO to Nation Gateway (NNG):** The NNG is an agreed hand over point between NATO and a Nation to allow information exchange for AIS (static) services. NATO is responsible to deliver the services to that point, whereas the Nation is responsible to provide connectivity and services from the NNG to the required location within the Nation. The NNG can be used for NS (future NR) and offers the option to include NS V2 services (SBC required). Additional security (i.e. firewalls on both sides) is required.
- **INF002NP - Network Interconnection Point (NIP):** A NIP is an agreed hand over take over point (Federated Mission Network compliant) between NATO and a Nation to allow information exchange for NRF, Exercises and Missions (this includes ships). NATO is responsible to deliver the services to that point, whereas the Nation is responsible to provide connectivity and services from the NIP to the required location within the Nation. The NIP can be used for (NRF) NU, (NRF) NR and (NRF) NS and offers the option to include V2 services (SBC required).
- **INF002LVAR - Local V2 Aggregation Router (LVAR):** An LVAR is deployed to enable delegated NMRs at the highest level of national command (e.g. CHOD / MOD) to access Secure Voice services. LVAR devices will be located within national NS infrastructures und national IT management. IPSEC tunnels will be created to connect to the NGCS. Nations are responsible for Level 1 support with Level 2 and 3 support from NCIA at best effort due to the services dependence on National Defence Network infrastructure.

NCI Service Flavours: The exact specification of this service is still under development but is likely to include:

- **INF002NCI – NCI Point of Presence[2]–** Core 40G, Enhanced 40G, Standard 40G and 5G. This flavour provides the latest service evolution for the POP service, and is a direct replacement for INF002 NLI, in regards to termination capabilities of medium bandwidth transmission services with links from 100 Mbit/s up to 40 Gbit/s. These PoPs are generally Common Funded and include multiple subsystems for Protected Core Access (PCA), Coloured Cloud Access (CCA) of multiple security domains: NU, NS, NR as well as Multi Media Access (MMA) for NU voice and video services.

Delivering capabilities on:

NATO Secret
NATO Restricted
NATO Unclassified

Service Prerequisites:

INF014 Enterprise Transmission Services (and NDNs for LVAR)

Underlying Services: INF046, OTH001, PLT008

Standard Service Support Levels:

Service Availability Target (SAT): 99.5% and must below INF014 SAT.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Availability for the NGCS POP Service is determined annually and is dependent upon enabling services and regional support arrangements. Availability target provided above is for 24/7 service, where the service option only in support hours will provide lower availability, to be agreed with the customer on the SLAs.

Service Cost / Price: The unit of measure for the service is per PoP.

Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate.

For the price details, see the Service Rate document.

INF003 Enterprise Internet Access Service

Service ID: INF003

Service Name: Internet Access Service

Portfolio Group: Infrastructure Services

Service Description: Enterprise Internet Access Service comprises of the provision and supply of secure web browsing connectivity to the internet, mail relay and mail security sanitation. Additionally this service supports collaboration and interoperability amongst any dependent NATO resources.

Value proposition: Enterprise Internet Access Service offers the user the access to the internet, enabling the user to conduct open source intelligence gathering, administration, welfare and many other activities to support their business needs.

Service Features:

- Downstream bit rates
- Upstream bit rates
- Monitoring from our Network Operations Centre
- High-speed access
- Secure access
- Corporate Web Proxying
- Corporate Internet DNS Service

Service Flavours: The service is available in the following flavours:

Standard Internet Access: is the standard internet provided across the enterprise based on the following principles:

- Access is controlled based on appropriate site categorisation, blocked for unappropriated site categories (Porn, Gambling, Storage on line, Etc.)
- Traffic of any kind is subject to inspection including SSL decryption as appropriate (exclusion for Banking, Health and Governmental institution)
- Exception to the above are organised by means of policy on user request approved by the local SSA

Anonymized Internet Access: is an internet access organised in a way that browsing result sourced from IP addresses are not attributable to NATO. Anonymisation is a data processing technique that removes or modifies personally identifiable information; it results in anonymised data that cannot be associated with any one individual or organisation (NATO in this case).

Available on:

NATO Unclassified
NATO Restricted

Service prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side).

Underlying Services: INF051, OTH001, SME005

Standard Service support levels:

	Availability Target	Restoration Period
In support hours	99.9 %	1 hour
Out of support hours	99.5 %	4 hours

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the table above.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is 1, meaning that the cost/price of the service is calculated on the enterprise total cost basis.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Impact on service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

CIS Security and Cyber report

Asset and Configuration Management reports

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

INF004 Infrastructure Virtualization Service

Service ID: INF004

Service Name: Infrastructure Virtualization Service

Service Type: Enabling

Portfolio Group: Infrastructure Service

Service Status: Available

Service Description: The Private Cloud and On-Premise Virtualization Service provides scalable and resilient compute resources on NCIA's Enterprise on-premise and private cloud infrastructure. This service handles all aspects of Virtual Machines (VMs) and physical servers lifecycle management, from initial provisioning and operating system installation to ongoing maintenance, including security patches availability, security hardening, performance monitoring, and 24/7 support.

Value Proposition: This service enables VM and server owners to host databases, application and other services without dealing with the complexity of underlying infrastructure. This service easily scales compute resources up or down in order to meet changing business needs and optimize costs. This service minimizes downtime with a redundant and highly available infrastructure delivered from strategically located datacenters. The shared infrastructure model offered by this service significantly reduces the Total Cost of Ownership (TCO) by lowering hardware costs, eliminating the need to manage physical infrastructure, and optimizing physical resource utilization.

Service Features

The Service offers the user the following:

- Based on proven, best-in-class enterprise hardware and software;
- Enterprise compute hardware and software procurement;
- VMware Hypervisor administration including hypervisor level security hardening per NATO NOS standards, hypervisor and firmware upgrades and hypervisor patching
- Resource pool architecture, consisting of vCPU, vMemory, and shared SAN or software-defined storage;
- Generally configured for high availability and dynamic resource allocation;
- Flexibility to modify resource pools generally without VM downtime;
- Continuous monitoring and optimization of resources allocation;
- Dynamic scalability of resources to meet evolving requirements;
- Supported operating systems:
 - Windows Server (A2SL approved versions only);
 - RedHat Linux (A2SL approved versions only);
 - Oracle Enterprise Linux (A2SL approved versions only);
- Operating system provisioning, upgrades and patching:
 - Deploying Microsoft Security Patches to Windows virtual machines or physical servers;
 - Deploying RHEL / OEL OS Security patches to RHEL / OEL virtual machines or physical servers;

- Deploying Emergency or Battle Short Patches to virtual machines or physical servers;
- Operating system patches deployment types:
 - *Automatic patching*: applied to servers automatically during maintenance windows;
 - *Manual patching*: made available to guest operating systems. Application owners are responsible to perform the install and initiate the system reboot.

Service Flavours:

- Load balancing web services; currently this is not enabled for all kinds of virtual machines.
- Deployment of custom Open Virtualization Format images (OVAs) on VMs (A2SL approved versions only);
- Deployment of A2SL approved operating systems on physical servers (requires strong justification).

Available only on Static Environments:

NATO Unclassified;
 NATO Restricted;
 NATO Secret;
 Mission Secret;
 Public Internet Access (PIA) Gateway.

Service Prerequisites:

- INF001 LAN Service;
- INF002 NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service;
- INF005 Infrastructure Integration Service;
- INF007 Infrastructure Storage Service;
- INF014 Transmission Service (WAN connection & bandwidth requirements);
- SEC011 Gateway Security Service.
- SEC014 Crypto Management and Logistic Support Service

Standard Service Support Levels:

Service Availability Target: 99%

Built-in High Availability provides uniform failover protection against hardware and operating system outages within the virtualized IT environment offered by this service. High availability allows:

- Monitor VMware vSphere compute devices to detect hardware and system failures
- Restart virtual machines on other compute devices in the cluster without manual intervention when a server outage is detected

- Reduce application downtime by automatically restarting virtual machines upon detection of an operating system failure

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0311	NATO Data Centre Virtualization
A3024	Deploying VMware vSphere

Service Reporting:

- Incident management reports based on ITSM tickets and trend analysis;
- Change management and ASI reports based on ITSM tickets;
- Additional service reporting requirements can be requested through the respective SLAs, which are subject to NCIA's cost and feasibility assessment.

Service Cost / Price:

The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF005 Infrastructure Integration Service

Service ID: INF005

Service Name: Infrastructure Integration Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Integration Service provides the underlying infrastructure network services that are required to have a working IT environment. It ensures the availability and capacity of the Data Centres at several locations. It ensures the availability and capacity of the Data Centres at several locations. As a part of IaaS (Infrastructure as a Service) INF005 builds the basement for the centralized IT Infrastructure and create the hardware level for other centralized services. The fields of activity of Infrastructure Integration Service are Space, Cooling and Power inside the centralized NCIA IT Infrastructure. Also Network Time Protocol (NTP) is part of the service flavour provided by Infrastructure Integration Service. INF005 is a non-customer-facing service and is a prerequisite for Infrastructure Virtualization Service (INF004) and Storage Service (INF007) and Backup Service (INF016).

Value Proposition: The Infrastructure Integration Service is essential for a proper functioning IT environment. We plan, implement and manage the centralized IT environment within the NCIA IT Infrastructure.

Service Features:

- **Space:**
 - Physical Security
 - Classifications Security
 - Space Optimization
 - Space Utilization
 - Sustainability
 - Integration (Rack and Stack)
 - Migration
 - Cabling
- **Power:**
 - Distribution / Modernization
 - Redundancy
 - Control and Monitoring
 - Assessment
- **Cooling:**
 - Air Distribution
 - Efficiency Assessment
 - Control and Monitoring

- Assessment

Service Flavours: The Service is available as a single flavour.

Available on: NATO Secret
Mission Secret
NATO Restricted
NATO Unclassified

Service Prerequisites: None

Standard Service Support Levels:

	Availability Target	Service Restoration Period
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The service rate for this service is included under the service rate of INF004 Infrastructure Virtualization Service. No separate charges apply for this service specifically.

INF006 NATO Enterprise Directory Service (NEDS)

Service ID: INF006

Service Name: NATO Enterprise Directory Service (NEDS)

Service Type: Customer Facing, Supporting, Enabling

Portfolio Group: Infrastructure Services

Service Status: Available

Service Description: NEDS provides the capability to share trusted identity information between different systems. The information on identities (e.g. people, post, organizations) are retrieved from different authoritative sources (e.g. APMS, Active Directory). NEDS is enabled to NATO enterprise (including NATO HQ) and is becoming the standard way to exchange identity information. Information are synchronised between different affiliate systems and automated workflows are in place, including provisioning and de-provisioning of User Accounts. NEDS serves the identity information through the NEDS native interface (such as LDAPS), as well as customized interfaces (such as Web Access, file based interface or SQL access).

Value Proposition: NEDS provides value to customers through the sharing of identity information across multiple identity stores, improving data quality while reducing the administrative burden on the connected systems. This ensures a coherent set of identity data from authoritative sources, while increasing the security posture of the NATO Enterprise.

Service Features:

Identity Management Data sources/consumers can make use of the NEDS native interface for retrieving or updating identity information using LDAP(S). Beside, tailored interfaces can be developed based on for instance SQL or file based connectivity.

Currently Affiliated Systems:

- **Automated Personnel Management System (APMS)** - provides a workforce and personnel database for all users at every level within the NATO Command Structure (Bi-SC).
- **SmartTrack** - NEDS provides identity attributes information in support of Configuration Management Database
- **ITSM (Remedy)** - NEDS provides identity attributes to the ITSM ticketing system, which enables the ITSM system to get information like name, organization, grade and account.
- **NATO Public Cloud (NPCL)** – NEDS acts like the single point of identity information provider in support of account provisioning.
- **Bi-SC Active Directory** – NEDS pulls the existing user accounts from Active Directory, and it pushes new user accounts into the Active Directory automatically.
- **NATO Network Control System (NNCS) Database** – NEDS pulls the Formal Military Messaging information such as Address Indicator Groups (AIGs), Signal Message Addressee (SMAs) / Plain Language Addressee (PLAs),

Routing Indicators (RIs), NATO Subject Indicator Codes (SICs). Also, NEDS enables these information to NNCS through a web portal.

The administrator of the subscribing affiliate can choose the authoritative attributes. NEDS may also connect to the additional authoritative affiliates.

Yellow pages - NEDS enables a portal for search function for the existing identity through a web browser. The browser retrieves the variety of information like name, telephone number, email-address, and office/room number.

Service Ordering and Request: Any new affiliation requests or change requests for existing affiliations must be submitted through CRF.

Service Flavours:

Identity Management: Each user has one identity which may come with several attributes (like last name, first name, organization units, security clearance level, post details, location & address, telephone numbers, credentials and email addresses on different networks, profile photo, etc.). When the affiliation is built, the identity data can be exchanged with NEDS, based on a signed synchronization agreement which depict the predefined attributes or filters.

Yellow pages - NEDS enables a portal for search function for the existing identity through a web browser. The browser retrieves the variety of information like name, telephone number, email-address, and office/room number.

Available on:

NATO SECRET

NATO RESTRICTED

NATO UNCLASSIFIED.

Service Prerequisites:

APP029	Military Messaging Handling Application Service
APP032	Personnel Management Application Service
INF004	Infrastructure Virtualization Service
INF005	Infrastructure Integration Service
INF007	Infrastructure Storage Service
WPS002	Enterprise Identity and Access Management
WPS003	Enterprise User License Service
WPS012	Workstream Collaboration Service

Standard Service Support Levels:

Service Availability Target: 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

- **Service Restoration:** Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) Restoration Time is 2(two) working days with 80% INC IN SLA Enterprise-wide

N.B. Service will be restored under the condition that underlying services are available. Priority Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

- **Service Reporting:** Service Reports will be based on the number of incidents (solved/failed), Service Request. Also availability figures will be populated from the service monitoring toolsets/features.

Available NCI Academy Training not covered by service cost: No training is available on the Agency's catalogue yet. There will not be any training for the end users since this is an enabling service.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Depending on the delivery of ON and PBN, the service unit of measure will be analysed and published.

INF007 Infrastructure Storage Service

Service ID: INF007

Service Name: Infrastructure Storage Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Storage Service is an underlying technical service that offers flexible, scalable, efficient and secure Storage Service primarily supporting INF004 and INF016 services. The Infrastructure Storage Service supports NCIA's enterprise on-premises and private cloud infrastructure by enabling the hosting of virtual machines, managing shared file systems, and storing backups. It is delivered through two main storage types ; block and backup in order to effectively meet diverse business requirements. .

Offering any end-user storage devices such as internal, external hard drives or flash memory-like devices is not in the scope of INF007.

Value Proposition:

- **Enterprise-Level Storage Backbone:** Provides a secure, scalable, and efficient storage foundation for mission-critical workloads across NCIA's enterprise infrastructure.
- **Optimized for Business Continuity:** Enables and support backup and restore operations with high availability, redundancy, and long-term retention through robust storage solutions.
- **Seamless Integration & Performance:** Delivers seamless storage integration with NCIA's private cloud and on-premises infrastructure, enhancing operational efficiency.
- **Dedicated Infrastructure Focus:** Concentrates on core storage infrastructure, excluding end-user storage services, to ensure reliability and performance for enterprise applications.

Service Features: The Infrastructure Storage Service is comprised of the following features:

- **Two-Tier Storage Offerings on Private Cloud & On-Prem:** Provides block, and backup storage, catering to diverse enterprise needs, including VMs, shared file systems (CIFS, NFS), and long-term retention.
- **High-Performance Block Storage:** Ensures fast, low-latency storage for virtual machines and databases, optimizing workload efficiency.
- **Enterprise Backup & Disaster Recovery:** Offers robust backup storage with defined retention policies to secure critical business data.

Service Ordering and Request:

Storage capacity requests for new or existing VMs are submitted through the ITSM toolset and assessed by the NISC Capacity Management Board.

Service Flavours:

- **File Share Services:** Delivers shared file system support (CIFS/NFS) for collaborative enterprise environments. (Access rights are managed by IKM officers and/or data owners not INF007).

- INF007 may also introduce the following Service Flavour offerings once the **ITM** project has successfully transitioned to operation in the respective locations:
 - **S3-Compatible Object Storage** – Enables scalable, cloud-compatible object storage for unstructured data and modern application workloads.
 - **VAAI (vStorage APIs for Array Integration)** – Enhances storage performance by offloading intensive tasks to external storage arrays.
 - **Cloud-Native Storage (CNS)** – Provides persistent storage solutions designed for containerized applications, ensuring seamless integration with Kubernetes environments.

Available only on Static Environment not DCIS:

- NATO Unclassified
- NATO Restricted
- NATO Secret
- Mission Secret
- Public Internet Access (PIA) Gateway

Service Prerequisites:

- INF001 LAN Service
- INF004 Infrastructure Virtualization Service
- INF005 Infrastructure Integration Service
- INF016 Infrastructure Resiliency and Protection Support Service
- INF002 NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service (WAN connection& bandwidth requirements)
- INF014 Transmission Service (WAN connection& bandwidth requirements)
- SEC011 Gateway Security Service (Firewall requirements)

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
Public Internet Access (PIA) Gateway

Service Prerequisites:

- INF001 LAN Service
- INF004 Infrastructure Virtualization Service
- INF005 Infrastructure Integration Service

Standard Service Support Levels:

Service Availability Target: 99%

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting:

Incident management report base on ITSM tickets and trend analysis.

Change management and ASI report based on ITSM tickets.

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

Service Cost / Price: The service rate for this service is included under the service rate of INF004 Infrastructure Virtualization Service. No separate charges apply for this service specifically.

INF012 SATCOM Service

Service ID: INF012

Service Name: SATCOM Service

Portfolio Group: Infrastructure Services

Service Description: The SATCOM Service provides bandwidth to remote customers unable to be supplied by terrestrial infrastructure. The SATCOM infrastructure provides state-of-the-art communications supporting deployed operations anywhere within NATO's area of responsibility. It does this with its own ground equipment and control systems, operating with satellite capacity leased from the national governments of Great Britain, France, Italy and the United States.

Value Proposition: The Service provides the following value and benefits:

- **Location:** SATCOM services allow the customer to extend their communications networks to anywhere within NATO's area of responsibility.
- **Scale:** The service is scalable to support a variety of different deployments in both size and complexity, ranging from one telephone circuit to a complete intra-theatre hub and spokes and backhaul to the static HQ.
- **High redundancy:** The static SATCOM infrastructure has significant redundancy and a low probability of failure.
- **High Availability and Security:** SATCOM uses a variety of methods to ensure that communications in a hostile electronic environment maintains a high level of availability and security. These methods include:
 - Frequency hopping modems
 - Hardened satellites
 - Beam-nulling satellite antennas
 - Beam-steering satellite antennas

Service Features:

- **Redundant anchoring using dispersed locations:** provides greater resilience and availability, plus space diversity.
- **Dynamic bandwidth allocation** using global QoS to set priorities. Links are transparent to NGCS network.
- **Hardened satellites at X-band:** increased ability to work in a hostile electromagnetic environment.
- **Beam-nulling and beam-steering satellite antennas at X-band:** increased ability to work in a hostile electromagnetic environment.
- **Anti-jam modems:** increased ability to work in a hostile electromagnetic environment.
- **Voice and data services:** Links are transparent to NGCS.
- **Inherently secure communications** through the use of closed networks and the ability to integrate with VPN, COMSEC and TRANSSEC services. Increases security and integrity of information.

- **One-stop-shop** for all satellite queries and issues: NATO's centre of excellence for all SATCOM matters.
- **Fully managed communications suite** from an organization that understands the needs of the military. Centralised management ensures continuity, efficiency and full systems visibility.
- **Anchor station manning:** minimum one person on shift at all times to ensure timely response to faults, events and changing situations.
- **Ability to react quickly to new requirements** and changing circumstances: SATCOM is set up to process requirements within the SLA agreed with ACO.

Service Flavours:

Individual deployment: Small, commercial handheld and portable voice and low-speed data communications

Individual operational deployment: hand-held, vehicle and ship-mounted UHF systems providing secure, narrow-band voice and data. (Please note that the TACSAT UHF devices are separately captured under the INF040 UHF TACSAT Radio Services)

Wideband deployment: transportable systems providing voice, video and data to deployed formations, complete with intra-theatre and backhaul SATCOM networks using X- or Ku-band satellites

Wideband secure deployment: transportable systems providing voice, video and data to deployed formations, complete with intra-theatre and backhaul SATCOM networks using anti-jam modems and hardened X-band satellites

Additionally the table below provides infrastructure or support options available under each flavour, which cater to a variety of deployment requirements.

Service Flavour	Options under the Flavour	Description	in units	Support level available
Individual deployment	Inmarsat	Small, highly portable secure and insecure voice and data communications for initial deployments		2 nd , 3 rd line
	Iridium	Handheld telephone-type communications		2 nd , 3 rd line
Individual operational deployment	NUCC controller maintenance	This is the hub of the TACSAT system, providing DAMA and IW capabilities to improve bandwidth efficiency		2 nd , 3 rd line
Wideband Secure deployment	X-band anchoring	4 sites with 10 antennas to anchor all of NATO's broadband satellite communications, including anti-jam. Includes EMP assets	332MHz SAL-2 and 84MHz SAL-3	SAA production, 3 rd line
	DCIS TSGT support	3 rd -line maintenance, repair and upgrade management	As requested	3 rd line

	DCIS DSGT support	3 rd -line maintenance, repair and upgrade management	As requested	3 rd line
Wideband deployment	SkyWAN operation and maintenance	Hub and spoke VSAT system, provided as VNC by LUX, currently used for NC2	2MHz, 8 terminals	2 nd , 3 rd line
	Melusina 2 administration	Administration of the LUX Ku-band VNC contribution	42MHz	3 rd line
	DCIS TSGT support	3 rd -line maintenance, repair and upgrade management	As requested	3 rd line
	DCIS DSGT support	3 rd -line maintenance, repair and upgrade management	As requested	3 rd line

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Underlying Services: OTH001, SME005, TRA002

Standard Service Support Levels:

	Availability Target	Service Restoration Period
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

N.B. Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0032	NATO SGS/SGT SAC Operator Maintainer
A0601	SATCOM Basic (048)
A4000	CCT200 SATCOM Terminal NATO Mission Iraq (NMI) Operator



Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF013 NATO CIS (VLF) Mission Support for Submarine Operations Very Low Frequency (VLF) Broadcast Service

Service ID: INF013

Service Name: NATO CIS (VLF) Mission Support for Submarine Operations Very Low Frequency (VLF) Broadcast Service

Portfolio Group: Infrastructure Services

Service Description: Very Low Frequency (VLF) Broadcast services provide Submarine Operating Authorities (SUBOPAUTH's) with robust, secure and timely message delivery within the NATO Area of Responsibility in order to ensure effective Command and Control of sub-surface forces.

Value Proposition: VLF is the primary means of communicating with submarines. The NCI Agency managed VLF network (provided under INF002 - NATO General Purpose Communication System (NGCS) Point of Presence (POP) Service) is a key enabler for connecting shore SUBOPAUTH's to VLF Broadcast Radiating Stations for subsequent message delivery to submarines.

The INF013 service provides hardware and software to compile broadcast routines utilising the Broadcast Control Authority (BCA), and to transfer traffic (broadcasts and Over the Air monitoring (OTAM)) between Broadcast Control Station (BCS) and Broadcast Radiating Station (BRS) Interface Devices. The BCS and BRS provides a live picture of the network status including; site status, keystore delivery and clear indication of system issues. The ability to pass remote Over the Air Monitoring to a distance site makes the BCS system extremely flexible for conducting submarine operations across NATO.

Service Features:

- Broadcast Control Authority (BCA)
 - Provides broadcast traffic at Mission Secret
 - System Administration Management
 - Hardware and Software solutions
 - Interfaces with crypto for secure communications
 - Interfaces with Military Message Handling Systems (MMHS)
- Broadcast Control Station (BCS)
 - Live connectivity picture
 - Broadcast Traffic Table management
 - Connection to NATO provided Broadcast Radiating Station (BRS) via the VLF network or to national transmitters via external lines.
 - Fully Redundant
 - Swap and replace solution
 - Facility to pass remote OTAM between sites
 - Group CHAT facility
 - Minimum operator involvement

- Broadcast Radiating Station (BRS)
 - Passes broadcast traffic to national transmitters
 - Utilises same hardware and software as BCS
 - Fully Redundant
 - Swap and replace solution
 - Minimum operator involvement
- NATO VLF WAN
 - NCI Agency managed dedicated IP network for NATO VLF BCS and NATO BRS Interface Device (INF002) is available as a separate service.
- Broadcast Support Site (BSS)
 - Provides test bed for system hardware and software validation and configuration changes
 - Training facility y providing operator and technical training for NATO VLF hardware and software.

Service Flavours: The Service is available as a single flavour, with the following options:

- Provision of Broadcast Control Authority
- Provision of Broadcast Control Station
- Provision of Broadcast Radiating Station Interface Device
- Provision of OTAM facility (receivers and demodulators)

Available on:

Mission Secret
NATO Unclassified

Service Prerequisites:

None

Underlying Services: OTH001, SME005

Standard Service Support Levels:

	Availability Target	Service Restoration Period
During Support hours	99.95 %	1 hour
Outside Support hours	99.5 %	4 hours

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF014 Transmission Service

Service ID: INF014

Service Name: Transmission Service

Portfolio Group: Infrastructure Services

Service Description: The Transmission Service provides the network backbone infrastructure over wired or wireless transmissions bearers in order to connect all NATO Enterprise Static CIS nodes under a common Protected Core Community (PCC), underpinning the Network Enabled Capability of NATO. The Service is largely outsourced to 3rd parties (Commercial Service Providers and/or National Defence Networks NDNs). It includes full life-cycle service management like service design, capacity management, configuration and change management, operational support and continual improvement and optimization.

Value Proposition: The Service enables the NATO Enterprise static wide area network and provide the primary means by which dependent services and capabilities reach geographically dispersed consumers and users.

Service Features: The Service provides high capacity and resilient transport network infrastructure, scaled to meet the data traffic needs for all NATO Enterprise CIS nodes and future-proofed for additional customer requirements. It ensures effective transport of services and data across NATO by means of a Protected Core Network. The Service is comprised of the following elements:

Wired: delivered by fibre optic cabling as part of contract with Telecommunications Service providers or National Defence Networks (NDNs) providers. Available bandwidths:

- 100 Gbps
- 1 Gbps or multiples
- 100 Mbps or multiples
- Lower bandwidth based on requirements, costs and geographical constraints

Wireless: provides additional capacity to link NGCS sites, where wired connectivity is not possible or efficient. Consists of links used to connect physically remote sites and come in the form of:

- Direct Line of Sight (DLOS): Microwave radio transmission equipment with directional antennas (100-400 Mbit/s), including CIP-67.
- Alternate Redundant Transmission (ART): Alternate bearer services in the form of commercial satellite connectivity, from commercial operators to provide increased availability and/or increased resilience to outages

Service Flavours:

NATO Enterprise Static CIS nodes: Wired and wireless service elements are designed and offered as a bundle

3rd Party CIS nodes: Selectable elements out of the existing Service Features

Standard KPIs/KQIs:

Availability: Subject to external providers' SLAs and support contracts.

Available on: This service has no security classification and is considered as unclassified.

Service Prerequisites: None

Underlying Services: OTH001, SME005

Standard Service Support Levels: Service Availability for the Service is determined annually and is dependent on external support contracts, enabling services and regional support arrangements.

Available NCI Academy Training not covered by service cost:

A0236	NATO Networking Infrastructure (CCNA R&S)
A0650	CCENT (ICND1)
A3046	Network Configuration and Troubleshooting
A3135	Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)
A3136	Implementing and Administering Cisco Solutions (CCNA)

Service Cost / Price: The unit of measure for the Service is 1 for Service Flavour of NATO Enterprise Static CIS nodes. For the 3rd party CIS nodes flavour, the unit of measure depends on the customer requirements and is calculated on an ad-hoc basis. The respective service provision cost is subject to external Service Provider contracts.

INF015 Broadcast, Maritime Rear Link and Ship-Shore (BRASS) STIV RMD Service

Service ID: INF015

Service Name: Broadcast, Maritime Rear Link and Ship-Shore (BRASS) System Test Integration and Verification and Reference Maintenance Diagnostic (STIV RMD) Service

Portfolio Group: Infrastructure Services

Service Description: The NATO Broadcast, Maritime Rear Link and Ship-Shore (BRASS) system is designed to support all NATO Maritime missions. It provides automated support for the NATO Maritime Surface Broadcast, the Ship-Shore and the Maritime Rear Link (MRL) HF communications networks. The System Test Integration and Verification and Reference Maintenance Diagnostic (STIV-RMD) facility replicates a minimal and representative BRASS operational site, mirroring the hardware and software components used in the BRASS Initial Core Capability (BICC), to the extent possible, with minimal additional hardware and software modules. The service includes all functions necessary to test and validate all services performed in an operational BRASS node. It is principally used for maintenance, testing and verification of BRASS software and its future implementations and is installed at Casteau Mons (SHAPE, Belgium), in NCIA facilities. The system can also be used for hands-on training of NATO/national BRASS personnel. The STIV-RMD facility interfaces the NGCS (NATO General Communication System) to connect to NCIA radio sites in The Hague and Staelduinen (NLD). The service is built from two nodes. One representing the standard BRASS node and the second allowing the simulation of the traffic up to the HF modem level. It is equipped with standard crypto units that are used in BRASS nodes and can be used in the simulation chains with unclassified traffic and crypto keys.

Value Proposition: The BRASS STIV-RMD facility allows testing of the key-streams transmitted/received by radios at the NCIA sites (HF TX in Staelduinen and the HF RX radio site in The Hague) without engaging assets required for military operations. The service design allows the simulation of the traffic without the need to use full radio equipment chains. The BRASS STIV-RMD facility is built in a manner similar to an operational system. The system processes, stores and disseminated unclassified data only and doesn't perform real operational activity, which makes STIV RMD a perfect tool to perform hands-on training for the NATO and national BRASS personnel.

Service Features:

- The system includes all functions necessary to test and validate all services performed in an operational BRASS node such as:
- Management of NATO/national Broadcasts, Ship Shore, MRL, MATELO and Point-to-Point circuits (STANAG 4285, STANAG 5066);
- Management of crypto equipment;
- Automatic storage and retrieval of message traffic handled in the centre;
- Remote control of the assets belonging to the system (including radio devices, antennae and communication links)

- The system includes the necessary hardware capacity and the full set of software tools required to maintain the BRASS software

Service Flavours:

The project 2015/OCM03074 “Provide BRE1TA Software and Beyond Line of Sight Access Point with Remote Monitoring Diagnostics and Training Capability” from Capability Package 9A0101 “Wireless Communication Transmission Services Other than SATCOM” is going to deliver the enhancement to the INF015 BRASS Broadcast, Maritime Rear Link and Ship-Shore (BRASS) STIV RMD Service. The Final Operational Capability is expected mid 2026 with the aim to fully replace the current service by 2027.

This project is intended to upgrade the BRASS Initial Core Capability (BICC) software to the BRE1TA (BRASS Enhancement 1 Target Architecture) standard and to provide reference system and remote monitoring and diagnostic capabilities in NCIA Mons. Additionally, holistic training capability will be made available at NCIA Academy. The software will be available to the Nations as the standard, common software for all BRASS implementations to replace the legacy BICC.

The current service will be enhanced with the following:

- The reference system for Beyond Line of Sight Access Point (BLOS AP) in Mons (SHAPE, Belgium). The BLOS AP will include the mirror node allowing the simulation of all the scenarios of communications between shore BLOS AP and ships/mobile units. The installation will replace the existing BRASS reference system;
- The system will be connected to 2 pairs of transmitting and receiving stations located in NCIA locations in Netherlands (TX in Staelduinen and RX in The Hague) and in MOD Portugal sites (TX in Penalva and RX in Fonte de Telha) allowing the real radio transmissions to ships and other entities or to close the skywave link between them for test purposes;
- BRASS IP Enhanced System (BRIPES) software that will provide new capabilities to the current HF radio communications users at sea including:
 - Formal Military Messaging according to STANAG 4406;
 - Informal SMTP messaging (e-mail) and JChat;
 - Web and data services;
 - Directory and mobility services;
 - Modern STANAG 5066 processor with Performance Enhancing Proxies to allow IP type of traffic over HF radio;
- Hardware HF Simulators allowing initial testing without the need for radio transmissions;

The service will deliver the tools to test interoperability of the national BLOS AP implementations on shore and upgraded ship installations without engaging operational assets. This will include testing of the BRASS IP Enhancement Deployable Kits for Standing Naval Force Flagships provided by UR 3442. It will ensure up to date software configuration

and patches for the Nations adopting BRIPES solutions. Finally, it will offer the training program and tools to the NATO and national operators at NCIA Academy in Oeiras.

Available on:

NATO Unclassified

Service Prerequisites:

None

Underlying Services: OTH001, SME005

Standard Service Support Levels:

Service Availability Target: 98.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF016 Infrastructure Backup Service

Service ID: INF016

Service Name: Infrastructure Backup Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Backup Service is an underlying technical service that offers secure, and automated backs-up and restores (B&R) capability for virtual machines (VMs) and server hosted files running on NCIA's Enterprise on-prem and private cloud infrastructure.

This fully managed backup service supports businesses and operation in order to minimize downtime, the risk and impact of data loss caused by failures, human errors or data corruption with centralized retention management, and reliable recovery options. NCIA SDMs and VM owners can benefit from automated backup policies tailored to their operational needs, supporting compliance, security, and seamless restoration capabilities in case of failures, data corruption, or accidental deletion.

Backup-Retention period may be specific to the different services and thus dependent on their specificities in terms of back-up and compliance requirements. The backup strategy for Customer Facing NCIA Services including retention time, backup type, frequency/schedule, recovery model, restore time objective (RTO), recovery point objective (RPO) and other requirements can only be defined after in-depth coordination and collaboration with the related NCIA SDMs or VM owners regarding their recovery objectives, acceptable risk, and overall business continuity objectives.

As an optional capability, VM Protection via Replication enables eligible VMs to be replicated to a Disaster Recovery (DR) site, enabling faster recovery and business continuity. This service is available upon request and subject to a suitability assessment and charge. This enhancement provides a failover mechanism for critical workloads, minimizing downtime and supporting rapid recovery in case of disruptions.

Value Proposition: This service strengthens business continuity readiness and operational resilience by utilizing secure, automated, and policy-driven backup and recovery for virtual and physical servers. Designed to support critical business processes, it enables improving the ability to:

- Comprehensive VM and Server-Level Protection: Prevent data loss of VM&server hosted files and increase availability, minimizing disruptions to core operations
- Business-Centric Recovery Planning: Customizable recovery objectives (RPO/RTO), backup schedules, and retention policies to align with business continuity requirements.

Service Features:

- Automated Backup & Recovery – Fully managed crash-consistent backup and restore for virtual machines (VMs) and server-hosted files.

- Data Retention Management – Structured backup retention policies enabling compliance, and secure data retrieval. (Note 1: Retention beyond one month is subject to assessment and may incur additional charges. Note 2: Long-term retention of VM backups should not be mistaken for Archive. INF016 is not responsible for archival services—retained backups are intended for recovery of VM and server hosted files, not regulatory or historical data storage)
- Customizable Backup Strategies – Tailored backup approaches, including:
 - Backup types (Full, Differential, Transaction Logs)
 - Scheduling & Frequency (Daily, Weekly, etc.)
 - Recovery Objectives (RPO/RTO) aligned with defined business needs.
- Reliable Restoration of VM and Server Hosted files – Enables recovery of previous copies to minimize downtime caused by failures, human errors, or corruption.
- Collaboration & Assessment – Backup strategies are defined in coordination with the related SDM and VM owners, ensuring alignment with mission-critical services and acceptable risk levels.
- Optional VM Protection via Replication (Service Flavour) – On-demand VM replication to a Disaster Recovery (DR) site, enhancing resilience and failover capabilities (subject to assessment of available storage, compute, WAN level capacity (bandwidth) and additional charges).
- Optional Application-aware backups: Increased consistency for mission-critical applications (e.g., databases, enterprise software) by capturing application state during backup.

Service Ordering and Request:

- New VM provisioning template on ITSM toolset (name can differ over time) contains backup requirements fields to be filled.
- Restore request are made by raising a Work Order on ITSM.
- NCIA SDMs and VM owners are recommended to coordinate their specific backup requirements and strategies with INF016 and relevant Platform, Application service before submitting their work order on the ITSM.

Service Flavours:

- Application-aware backups : Available upon request only. Requesters might be charged depending on capacity and eligibility.
- VM protection via replication: Available upon request only. Requesters will be charged depending on capacity and eligibility.

Available only on Static Environment (not DCIS):

NATO Unclassified;
NATO Restricted;
NATO Secret;
Mission Secret;
Public Internet Access (PIA) Gateway

Service Prerequisites:

- INF005 Infrastructure Integration Service (DataCenter floor, rack space, power, cooling requirements)
- INF007 Infrastructure Storage Service (Storage Capacity and storage-level replication requirements)
- INF004 Private Cloud and On-premise Virtualization Service
- INF001 LAN Service (Wired LAN connection requirements)
- INF002 NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service (WAN connection& bandwidth requirements)
- INF014 Transmission Service (WAN connection& bandwidth requirements)
- SEC011 Gateway Security Service (Firewall requirements)

Underlying Services: SME005

Standard Service Support Levels:

Service Availability Target: 99.0% Availability

Service Restoration: This service is not a customer-facing service. It is an underlying technical service designed to enable, help and support NCIA SDMs and VM owners to fulfill their VM restoration requests (fully or partially)

- 1- VM Failover to a Disaster Recovery (DR) Site: Failover time depends on replication frequency (RPO), network performance, storage speed, and VM complexity. With continuous replication, recovery is near real-time, often completing within several minutes. Actual failover duration varies based on system configurations and infrastructure readiness.
- 2- Restore from backups: Restoration time depends on data volume, storage location, network performance, and system workload. Recovery can range from minutes to several hours, depending on the complexity of the request and available resources. Actual recovery duration may vary based on infrastructure conditions and priority levels.

Restoration capabilities of an entire NCIA service or application ecosystems including all interdependent VMs, applications, databases, and other components falls outside the scope of this service. While individual VMs and their associated data can be restored, ensuring full service functionality post-recovery remains the responsibility of the service owner and may require additional configuration, application-specific recovery steps, or dependency management.

Backup data restore 2 working days	Backup data restore times depending on size/type of data
Conditions: - Customer IKM plans for data retention scheme	No hot backup standby No IKM plans No joint NCIA-Customer tests

- Tested RPO/RTO with Application Owner - Network bandwidth/latency sized - Tested Customer BCP - Off-site immutable backups	

NCIA SDMs and VM owners should factor in their own service recovery planning to ensure complete operational restoration beyond VM and data recovery. They are recommended to define end-to-end service recovery strategies that align with business continuity objectives and coordinate with INF016 and relevant Platform, Application and services.

VM backup retention: By default, the data retention period is one month. However, upon request and coordination with the data owner, backup copies can be kept for a longer period.

Service Reporting:

- There is no standardised service reporting due to complexity of backup environment.
- Incident management report base on ITSM tickets and trend analysis
- Change management and ASI report based on ITSM tickets
- Additional service reporting requirements can be requested through the respective SLAs it may be subject to suitability assessment and additional service fees.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The service rate for this service is included under the service rate of INF004 Infrastructure Virtualization Service. No separate charges apply for this service specifically.

INF020 DCIS – Deployable CIS Equipment Pool (DCEP) Service

Service ID: INF020

Service Name: DCIS – Deployable CIS Equipment Pool (DCEP) Service

Service Type: Enabling Service

Portfolio Group: Infrastructure Services

Service Status: Available

Service Description: DCEP consists of standard desktop terminal equipment that provides Communications Information Systems (CIS) Services to support the end user in the deployed environment. This equipment includes classified and unclassified workstations and laptops, classified (VoSIP) and unclassified (VoIP) telephones, projectors, printers, scanners, multi-function devices (MFD), VTC terminals and workstations with multi-screen capability. DCEP also contains an SLA specific amount of user equipment to support the Core Geographical Information Services (Core GIS) user community.

The service rate includes the cost for shipping multi mission DCEP equipment between the level 3 storage/repair facility and Customer peacetime locations, including the rotation of mission assigned equipment between Customer locations when no return to repair centre is required.

INF020 funding covers the level 3 maintenance, repair and replacement of faulty equipment therefore assuring the availability of the service at NCISG NSBs and NCI Agency CSSC.

LOG005 service funds the DCEP exercise support; preparation, deployment shipping, re-deployment shipping, level 3 testing, repair costs, cleaning and storage.

Operational tasking and assignment of all assets within the Service is the responsibility of the ACO J6 Cyber Operations Centre. This includes the allocation of DCEP starter packs to NCISG Standby DCIS Systems to pre-approved quantities.

Value Proposition: DCEP is a fully common funded DCIS capability that is available for use by the entire NATO Command Structure in support of Missions and the Medium Term Exercise Plan (MTEP).

This Service provides all hardware to extend NCI Agency Services hosted on DCIS NDDs and/or MIR to the Users community assigned to the Mission and Exercise Domains as per the Customer's business needs.

This service is aligned to the NATO Digital Backbone concept and supports multi Domain Operations at the strategic centre and the tactical edge depending on the service delivery point.

Management: The Provider includes Service Management support to the customer, as well as being the primary NCI Agency interface and initial point of contact with the customer for in

year execution of the services in accordance with the Service Level Agreement (SLA). The Service Management support includes the management and coordination of service deliverables across all NCI Agency entities.

Service Features:

Service Delivery Management (SDM): DCIS services are specific with the requirement for close coordination between Service Provider and the Service Operator. For that purpose, Service Delivery Schedule and Change Management Plan as planning and coordination tools are used and updated on a monthly basis. SDMs also provide Service Availability Management and Service Obsolescence Management Reports.

Obsolescence Management have been included within the INF020 Service Rates.

Service Provision: DCEP Service provides end user devices that can connect to MS, NS and NU domains for the deployed HQ staffs. In addition, DCEP service provides the NDD DCIS operator (crew) and DCIS system administration laptops.

End User Device connection to and disconnection from the DCIS domain is via an ITSM Service Request submitted to the Enterprise Service Operation Centre.

DCEP Service Maintenance:

- Level 1 and Level 2 equipment maintenance is conducted by the Customer at Peace Time Location (PTL) or deployed.
- The Provider delivers Centralised level 3 maintenance at CSSC Brunssum, at DCEP PTL or deployed locations.
- Wherever possible, DCEP level 3 maintenance will be outsourced to industry partners to enable NCIA resources to perform increased Change Management activities to support tailored mission requirements.
- The DCEP Service does not include IT consumables to the DCIS user. Consumables items, for example, printer toner, printer paper, batteries, cleaning products, headsets are the responsibility of the Customer and should be procured locally.

Service Flavours:

CIS Assets/Services: Standard DCEP Assets and Quantity		Min Specifications	Standard Ancillaries	Remarks
Laptop (INF020-1)	3,300	Dual Core Processor, 8Gb RAM, 100Mbps NIC, HD Graphics, 256Gb HDD/SSD, WIN 11 compatible with Windows Experience Index (WEI) Value > 4 on Processor, Disk Drive, Graphics and RAM	Power Supply	Hardware only - Enables user access to Classified and Unclassified data networks and services. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline
Work Station/ Computer (INF020-2)	1,300	Dual Core Processor, 8Gb RAM, 100Mbps NIC, HD Graphics, 256Gb HDD/SSD, WIN 10 20H2 compatible with Windows Experience Index Value of 4 or greater on Processor, Disk Drive, Graphics and RAM	Power cable, monitor, video cable, keyboard, mouse	Hardware only - Enables user access to Classified and Unclassified data networks and services. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline

Monitor (INF020-3)	2,750	20-24" colour monitor, 1600x900 resolution with range of VGA, DVI, DP, HDMI output options, WIN 10 20H2 compatible	Power cable, video cable	Hardware only - Enables users to have single and dual screen monitors on workstations and laptops on Classified and Unclassified networks. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline
Printer/ MFD (INF020-4)	750	A3/A4 Colour or Black & White Laser printer. Network or Stand Alone options via RJ45 or USB connectivity, WIN 10 20H2 compatible	Power cable, 1 set toner cartridges, USB/Network cable	Hardware only - Enables users to Print / Copy / Scan from A4 B/W up to A3 colour. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline
Scanner (INF020-5)	60	A4 Colour, 2400x2400 DPI, WIN 10 20H2 compatible	Power cable, USB cable	Hardware only - Enables users to scan A4 colour copies on Classified and Unclassified networks. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline
VoIP Phone (INF020-6)	2,150	CISCO 7900 and 8400 series VoIP and VoSIP telephones. 100Mbps RJ45 or FO connectivity	Power cable (if required), network cable	Hardware plus CISCO ios only - Enables user access to classified or unclassified telephony services. Configuration is provided by NCIA as system is configured from Node State to Mission State
VTC Equipment (INF020-7)	45	Polycom Video Teleconference System POLYCOM, REAL PRESENCE, GROUP 500-720P	As per System manuals	Hardware plus Polycom RealPresence VTC software - Enables user access to Classified and Unclassified Video Teleconferencing services. Configuration is provided by NCIA as system is configured from Node State to Mission State
Projector/ Beamer (INF020-8)	120	1500LM, 1920X1200, 16:9 aspect ratio, c/w range of AUDIO/HDMI/RCA/VGA/USB output options	Power cable, video cable	Hardware only - Enables conference room and briefing room services to be displayed
Projecting Screen	80	180cm x 180cm screen	Transit tube	Hardware only - Used with projector/beamer
Switch (INF020-9)	270	Full duplex, Layer 2 OSI device, 24 or 48 x 100Mbps access ports, 2 or 4 x 1Gbps uplink ports, WIN 10 20H2 compatible	Power cable	Hardware plus CISCO ios only - Provides Layer 2 access level connectivity for end user Data devices on Classified and Unclassified networks. Configuration is provided by NCIA as system is configured from Node State to Mission State
Fibre Reel (INF020-10)	270	Tactical fibre optic, 250 meters, single mode duplex.		Hardware only tactical fibre cable. HMA tactical connectors, single mode 9/125 micron, 250 metres on reel.
KVM Switch (INF020-11)	1000	Tempest level C. Supports up to 2 host computers and 2 displays. Data leakage prevention between connected computers		2 nd Gen Universal, secure KVM switch, 2-port dual head
CIS Assets/Services: Core GIS DCEP Assets¹		Min Specifications	Standard Ancillaries	Remarks
Core GIS Kit: Generation 1/3 (INF020-12)	8	DELL Precision 3620, Dual Core Processor, 8Gb RAM, 1000Mbps NIC, HD Graphics, Tempest C, Removable 500Gb HDD, WIN 10 20H2 compatible	Transport case, Power supply, keyboard, mouse	Hardware only - Enables user access to Core GIS data networks and services. Software/drivers are provided by the Customer as per current NRF Windows Core GIS Baseline
	16	23.8" HP Elite Display E240 colour monitor, WIN 10 20H2 compatible	Power and video cables	Hardware only - Enables users to have single or dual screen monitors on Core GIS workstations. Software/drivers are provided by the Customer as per
		HP M880Z A3 Colour Multi-function printer. Network or Stand Alone options via RJ45		

¹ Core GIS assets are included in the DCEP portfolio of individual equipment items but are designed to be deployed only as complete Core GIS kits.

	6	or USB connectivity, WIN 10 20H2 compatible	Power cable, 1 set toner cartridges, USB / Network cable	current NRF Windows Core GIS Baseline
	6	HP Designjet T830-36 A0 Colour plotter. Network or Stand Alone options via RJ45 or USB connectivity, WIN 10 20H2 compatible	Power cable, 1 set ink cartridges, USB / Network cable	Hardware only - Enables users to Print / Copy / Scan from A4 B/W up to A3 colour. Software/drivers are provided by the Customer as per current Core GIS Baseline
	6	HP Designjet T520 A1 colour plotter. Network or Stand Alone option via RJ45/USB, WIN 10 20H2 compatible	Power cable, 1 set ink cartridges, USB / Network cable	Hardware only - Enables users to Print up to A0 colour. Software/drivers are provided by the Customer as per current Core GIS Baseline
	6	Disk Array, Synology DS918+, 4 bay, 2.5/3.5", ESATA/2X RJ45/USB 3.0, INTEL CELERON J3455 2.3GHZ, 4GB RAM, WIN 10 20H2 compatible	Power cable, 1 set ink cartridges, USB / Network cable	Hardware only - Enables users to Print up to A1 colour. Software/drivers are provided by the Customer as per current Core GIS Baseline
	4	External Hard Disk Drive, 3.5", USB 3.0, 8TB, SEAGATE Backup Plus Hub, 160MBPS	Power cable, USB / Network cable	Hardware only - Enables users to externally store, backup and transfer data inside or outside of the network. Software/drivers are provided by the Customer as per current Core GIS Baseline
	24		Power cable, USB / Network cable	Hardware only - Enables users to externally store, backup and transfer data outside of the network. Software/drivers are provided by the Customer as per current Core GIS Baseline
Core GIS Kit: Generation 2 (INF020-13)	14	Dual Core Processor, 16Gb RAM, 100Mbps NIC, HD Dual Screen Capable Graphics, 512Gb HDD/SSD, WIN 10 20H2 compatible.	Transport case, Power supply, keyboard, mouse	Hardware only - Enables user access to Core GIS data networks and services. Software/drivers are provided by the Customer as per current NRF Windows 10 Core GIS Baseline
	28	23.8" HP Elite Display E240 colour monitor, WIN 10 20H2 compatible	Power and video cables	Hardware only - Enables users to have single or dual screen monitors on Core GIS workstations. Software/drivers are provided by the Customer as per current NRF Windows Core GIS Baseline
DF BoB	18	Full duplex, Layer 2 OSI device, 24 x 100Mbps access ports, 2 x 1Gbps uplink ports	Power cable	Hardware plus CISCO ios only - Provides Layer 2 access level connectivity for end user Data devices on Classified and Unclassified networks. Configuration is provided by NCIA as system is configured from Node State to Mission State
Media Convertor	508	Range of 10/100/1000Mbps, RJ45 to LC/SC/SFP	Power supply	Hardware only - Enables conversion of CAT5e/CAT6 copper cable to Multimode Fibre Optic cable
Webcam	150	2.0 Megapixel, Wide Angle 1280x1024 resolution, HD webcam with USB IP connectivity and built-in microphone		Hardware only - Enables user access to video and audio services on workstations and laptops.

				Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline

Configuration Changes:

- Major – Defined as a significant change to the service, such as complete replacement of all or majority of key configuration items. Major Changes are outside of the scope of the service and are managed through the NATO Security and Investment Program (NSIP).
- Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, hardware updates, security updates, and patches and replacement of defective equipment. Minor Changes are conducted continuously throughout the lifecycle of the Service and are undertaken by the Provider without affecting operational availability.

Service Prerequisites: User provided qualified operators.

Underlying Services: OTH004, SME005

Standard Service Support Levels:

Service Availability Target: In accordance with the stipulations of the service provisioning agreement and based on the Customer requirements.

Service Restoration Period: In accordance with the stipulations of the service provisioning agreement.

Service Cost / Price: The unit of measure for the Service is per item.

INF023 Contingency Network Service

Service ID: INF023

Service Name: Contingency Network Service

Portfolio Group: Infrastructure Services

Service Description: The Contingency Network Service manages provisioning and delivery of the contingency network connections, encompassing lifecycle stages from requesting the network connections until their retirement in an orderly and well-defined fashion. It comprises of the provision of simple network connections, normally used as ship connections or simple deployable asset reach-back connections for deployable network services in operations and/or exercises. The Service is available only to non-common funded customers of the NCI Agency.

Value Proposition: The Service enables an efficient establishment of temporary connections to the NATO Enterprise network and a temporary access to various NCI Agency IT services.

Service Features: The Service streamlines and tracks all the essential network service-provisioning activities such as requesting, funding/eligibility validation, design, configuration management, implementation, testing, and service operation.

Service Flavours: The Service is available in two flavours:

1. Establishment/modification of a contingency network connection;
2. Activation/deactivation of an existing contingency network connection.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels: N/A

Available NCI Academy Training not covered by service cost:

A3046	Network Configuration and Troubleshooting

Service Cost / Price: The unit of measure for the Service is Per Connection. Price details available in the Service Rate document.

INF028 ACCS Sensor Integration Module (ASIM) Service

Service ID: INF028

Service Name: ACCS Sensor Integration Module (ASIM) Service

Portfolio Group: Infrastructure Services

Service Description: The ACCS Sensor Integration Module (ASIM) is an information conversion service that facilitates the integration of civilian and military sensors with AirC2 systems like ACCS (APP050) or MASE (APP053). ASIM enables this integration of legacy civilian or military air defence sensors by translating a variety of sensor formats to an STANAG 5535/ADatP-35 or EUROCONTROL ASTERIX conform protocol as used by the AirC2 system.

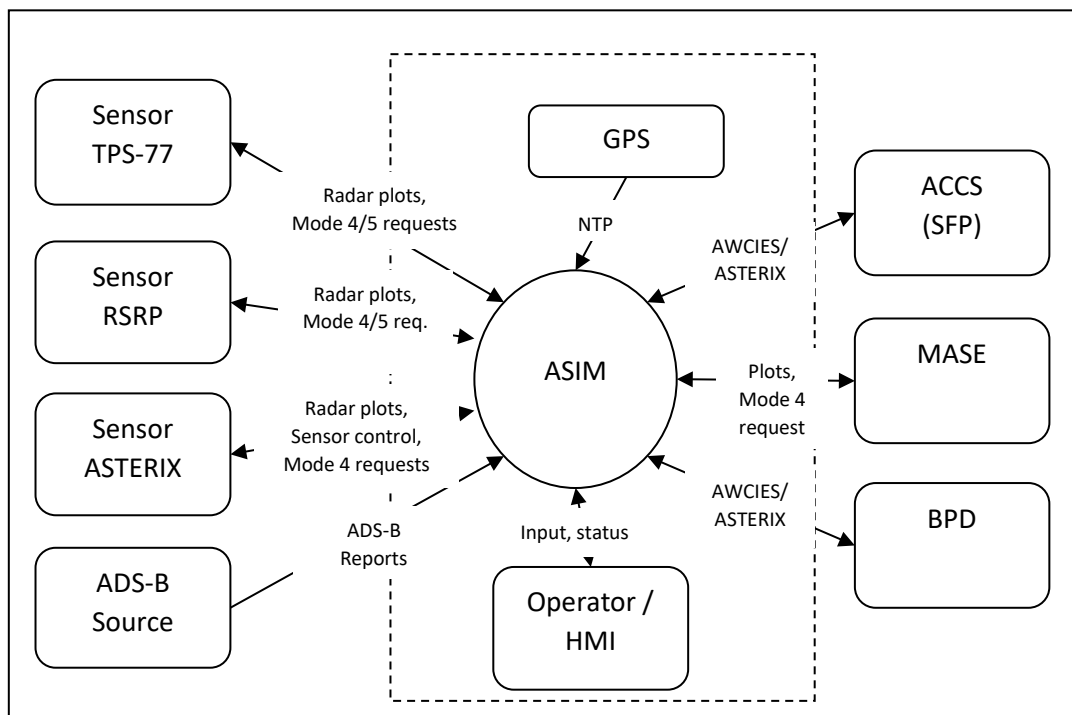
ASIM receives and converts sensor data, i.e. plots, strobes and radar status messages into equivalent ADatP-35 or ASTERIX conform messages and forwards this to the AirC2 system processing when applicable. Working the opposite direction as well, radar control and status information from AirC2 systems is translated respectively and forwarded to the connected sensors. Additionally, ASIM automatically provides sensor status data required by ACCS to declare the sensor link operational.

Value Proposition: ASIM Service provides a standard solution for interfacing non-compliant sensors with AirC2 ACCS (APP050) and MASE (APP053). The translation and exchange of data is fully configurable, automated and does not require operator attention. ASIM enables data to be monitored and controlled while sensor and control data can be recorded, replayed and dumped in real-time for quality analysis.

Service Features:

- ASIM connects legacy sensors with ACCS and MASE and provides target reports.
- Radar control actions from the ACCS/MASE operator are translated into sensor-specific messages, when applicable. I.e. currently Mode 4 and Mode 5 requests;
- The exchange of data is fully automated and does not require operator attention.
- The ADatP-35 and ASTERIX data into and out of ACCS or MASE can be recorded, replayed and dumped in real-time for data reduction and analysis;
- Redundancy as required for ACCS is supported;
- Safety related events are also forwarded to ACCS by ASIM as radar failure reports.
- Sensor and control data translation with a minimum latency and throughput not less than what is required for ACCS or MASE;
- In principle, ASIM appears to both ACCS/MASE and sensor as a transparent system. However, if target reports have an inconsistency between time and azimuth (which can lead to reduced tracking performance of the connected C2 system), ASIM is able to reduce this error based on reference data from the sensor.

The figure below outlines ASIM in a typical use case:



Supported configuration

- ASIM typically consists of two servers able to separate the sensor interface from the AirC2 system interface. This two-server configuration also supports to handle security levels differences between sensor groups and the AirC2 system.
- A boundary protection system such as the Application Layer Firewall for Sensors and Flight Plans (ALF-SFP – SEC022) can be integrated with the ASIM installation to protect system security boundaries from cyber threats.

Supported sensor/interface standards:

ASIM is STANAG 5535/ADatP-35 compliant towards the sensor and the AirC2 system and supports various sensor data formats inclusive JASR8, RMP, DDL, (A)S29, RAT31DL, FPS 117, TPS77, HADR, CD2, RSRP, S743D, AWCIES, T101, Cardion, T92, SRT and EUROCONTROL ASTERIX (various).

Other hardware, software and CIS details

- Uses NCI Agency (NPC) Integrated Secure platform (NISP) as a secured Solaris OS platform
- X86 or SPARC based server HW able to run NISP/Solaris, NOTE: NISP documentation provide a list of recommended HW

Service Flavours:

ASIM supports service the following service flavours:

- **NCS wide NATO ASIM** single SW baseline maintenance and In-Service-Support (ISS). The NATO ASIM SW baseline maintained with this service flavour is a prerequisite for all other service flavours.

- **Single ASIM configuration**, direct interfaces to sensor data and the ASIM servers are installed at a single location, usually at the ACCS location.
- **Split ASIM configuration** supports geographical separation of the direct sensor interfaces from the ASIM server connected directly to ACCS. This also supports that multiple remote sensor interface servers can connect to one server which provides the data to ACCS. This ASIM service flavour might be used to build up sensor networks managing the sensor data distribution between multiple sensors, AirC2 and ATC centres.

These two service flavours can be combined with an Application Layer Firewall for Sensors and Flight Plans (ALF-SFP – SEC022) to protect to protect system security boundaries against cyber threats.

Available on:

NATO Unclassified for handling civilian sensor data;
 NATO Confidential for handling military sensor data and
 NATO Secret for directly interfacing with the AirC2 system.

Service Prerequisites:

PLT013 (former APP051) NATO Integrated Secure Platform (NISP) platform service – mandatory – provides the secured operating system platform for hosting the ASIM server applications.

SEC022 – Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service – optional – provides boundary protection serves for connected AirC2 systems.

ASIM Hardware, software and connection requirements:

- Serial to IP network converter for serial sensor data;
- Sensor data available as serial data or at IP network level;
- IP interface as part of the ACCS or Air C2 system
- Server hardware compatible to run PLT013 - NISP and authorized to host the ASIM at required security level.
- Network infrastructure

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

- Belgium +32 65 44 3177
- Netherlands +31 70 374 3177
- Italy +39 081 721 3177
- Germany +49 282 4978 3177
- USA +1 757 747 3177
- For NATO HQ +32 02 707 5858

Service Requests:

To request the PLT013 – NISP Service, please complete the Customer Request Form and contact NCI Agency through the submit function included in the form following the link below.

https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

Functional unit	Service Level Target (availability)	Performance Thresholds
ASIM in single and split configuration	99.5%	30 ms delay for passing data between sensor and Airc2 system

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1010	ASIM System Administrator

Service Cost / Price: The Service delivery cost for each flavour is charged in accordance with specifically arranged conditions of the Service delivery.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
INF028	ACCS Sensor Integration Module (ASIM) Service	NCS wide ASIM software baseline maintenance and In Service Support (ISS)	1
INF028	ACCS Sensor Integration Module (ASIM) Service	Single ASIM configuration	1
INF028	ACCS Sensor Integration Module (ASIM) Service	Split ASIM configuration	1

INF029 NATO High Frequency (HF) Support Service

Service ID: INF029

Service Name: NATO High Frequency (HF) Support Service

Portfolio Group: Infrastructure Services

Service Status: Available

Service Description: The High Frequency (HF) Support Service is mainly provided via NATO BRASS (Broadcast, Ship-Shore) system, which is designed to support all NATO Maritime missions. The Service provides automated support for the NATO Maritime Surface Broadcast, the Ship-Shore and the Maritime Rear Link (MRL) HF communications networks and timely, accurate and reliable command and control communications and information exchange with NATO message switching and distribution capabilities.

There are NATO and nationally owned BRASS stations. National stations offer BRASS services to NATO based on Memoranda of Understanding signed with ACO. During the development, implementation and in-service support of NATO BRASS, NCI Agency has gained invaluable knowledge and is offering:

- Budgeting and financial mechanism to manage NATO funds granted for BRASS services delivered to NATO by Nations.
- In service support to BRASS Automated Control and Management Systems (ACMS).
- Support for BRASS Initial Core Capability (ICC) software.

Value Proposition: The HF Support Services offered for BRASS System provide:

- Proficient budgeting and financial structure in place with know-how of NATO procedures.
- Long experience gained during the in-service support of NATO BRASS sites.
- Expertise on the BRASS ICC software supported by the capabilities of the BRASS System Test Integration and Verification and Reference Maintenance Diagnostic (STIV RMD) facility located in NCIA Mons.

Service Features: The main features of NATO HF Support Services are:

- Existing budgeting and financial mechanism to manage NATO funds granted to pay for BRASS services delivered to NATO by Nations. In the past, NCIA managed funds for HF services delivered by Portugal to NATO and may provide similar support to ACO in case of Nations offering BRASS services to NATO based on service provision approach.
- In service support to BRASS Automated Control and Management Systems (ACMS). NCIA was managing the NATO ACMS nodes and HF stations before they were handed over to the Host Nations. NCIA supports the NATO ACMS in Northwood.
- Support for BRASS Initial Core Capability (ICC) software for the Nations that use it and may decide to use it in the future. The software baseline and source code and documentation is available for free to NATO nations. BRASS ICC software support and maintenance activities are performed in the NCIA BRASS System Test

Integration Verification Reference Maintenance and Diagnostic Facility (STIV RMD).

Service Flavours: This Service is available as a single flavour.

Available on: NATO Unclassified

Service Prerequisites: None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF034 Recognized Air Picture (RAP) Dissemination Service

Service ID: INF034

Service Name: Recognized Air Picture Dissemination Service

Portfolio Group: Infrastructure Service

Service Status:

L1DDN flavour: Available

Secure RAP flavour: Pipeline

Service Description: The Recognized Air Picture (RAP) Dissemination service primarily provides the infrastructure for transporting unencrypted Link 1 Data from the originating head end over NGCS network to the terminating tail end where the Link 1 Data is required. The Service is defined as the provision of infrastructure assets and capacity that enables the user to establish defined point-to-point connectivity. Secure RAP flavour is yet to be fully defined once the pipeline phase has completed. Secure RAP is geared towards providing the transporting of secure Link 1 Data and other required protocols references in Minimum Military Requirements (MMR) from the customer and AIRCOM mission.

Value Proposition: The Service is an integral component enabling the simultaneous transport and distribution of the Link 1 Data the Command and Reporting Centres (CRC), Combined Air Operations Centres (CAOC), and the Static Air Defence Centre (SADC), as well as for cross border connections CRC-to-CRC. Simultaneously, the service also enables the transport of Air Command and Control System (ACCS) data and Voice Loop (VL) services. Link 1 data enables the production of Recognized Air Picture (RAP), which, along with ACCS and VL are critical to the mission of AIRCOM.

Service Features: The L1DDN flavour services are available in the black domain of NGCS with the extended infrastructure elements to the CRC locations. L1DDN enables the transport of unencrypted Link 1 data, VL and ACCS data delivery. Secure RAP shall enable the secure transport of Link 1 data and ACCS data delivery.

Service Flavours:

L1DDN – enables the transport of Link 1 data between National CRCs and enables X-Border interconnections for same data exchange. The data exchanged and transported through the L1DDN is represented by Tactical Data Link (TDL) Link 1, operational Voice Loop services, and in some specific cases ACCS data. The Service is provided by leveraging and having dependencies on the capabilities delivered via NATO General Purpose Communication System (NGCS) available at the national NGCS Point of Presence (POP) and the National Defence Networks. The L1DDN is operational across all 30 NATO Nations, with presence and interconnections¹.

Secure RAP – distribution capability currently being implemented. A number of sites are planned start to distribute their Link 1 data or similar protocols via the secure links.

¹ As defined in AD 80-7 Vol III

The other will be integrated as the implementation project progresses in the following years. L1DDN should be decommissioned after the Secure RAP distribution is fully operational.

Available on:

L1DDN – NATO UNCLASSIFIED
Secure RAP – NATO SECRET

Service Prerequisites:

L1DDN flavour:

- INF014 Transmission Service;
- INF002 NGCS PoP Service;
- Transmission services via commercial or NDN providers between the CRC and the NGCS POP in the Nation.

Secure RAP flavour:

- INF014 Transmission Service;
- INF002 NGCS PoP Service;
- Transmission services via commercial or NDN providers between the CRC and the NGCS POP in the Nation.
- Pico PoP/POP required at all endpoints.

Standard Service Support Level:

Hours of support	24h/7d for CSD, 8h/5d for SLS/TLS

Service Availability Target: Service Availability for the Service is determined annually and is dependent upon enabling services and regional support arrangements. Service availability cannot be higher than the one of any of the enabling services.

Service Restoration:

Response time	1 hour
Restoration time	1d (critical/high), 3d (medium)

Available NCI Academy Training not covered by service cost:

A3046	Network Configuration and Troubleshooting
A3136	Implementing and Administering Cisco Solutions (CCNA)

Service Cost/Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF035 DCIS – Deployable CIS Nodes Service for Land Based Users (LBU)

Service ID: INF035

Service Name: Deployable CIS Nodes Service for Land Based Users (LBU)

Portfolio Group: Infrastructure Services

Service Description: This Service provides Standardised and Certified Deployable Communication and Information Systems (DCIS) Nodes. The Service provides the infrastructure and platform for a deployable CIS capability with inherent characteristics of modularity, scalability, sustainability, and interoperability. Each customer can adapt the Service to meet specific operational requirements through selection of the required workplace and application services. The customer can select those services from the workplace and application services sections of the Customer Costed Service Catalogue.

The Service includes service monitoring and reporting. This service has been upgraded in 2024 with the addition of enhanced cyber defence capability.

Value Proposition:

In peacetime location the service enable NATO to demonstrate a high readiness posture.

When deployed, the services are aligned with the NATO Digital Backbone concept to enable NATO Warfighters from the strategic centre to the tactical edge to make the timely decisions for mission success.

The customer will have direct access to the Agency Service Management team for Deployable CIS and will be supported as described in the OTH004 Service Description.

Service Features:

Included NCI Agency Services: listed for each specific flavour in the Service Flavours section.

Included NCI Agency Services correspond with standard NCI Agency services, as described in respective service definitions. However, due to deployable nature of the entire DCIS Nodes Service, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences will be described in detail within the respective service provisioning agreement (i.e. SLA, SSP, TA, etc.). Delivery cost of these services differs from the standard service rates, and it is entirely included within the DCIS Nodes Service cost.

The DCIS Nodes Service can host a variable number of Users (workplace services) and Application Services (Functional Area Services, FAS). The customer can select the specific requirements for the workplace and application services using the service catalogue, at additional cost.

Included in the service rates are the workplace services and applications for the system administrators to perform their duties.

Included CIS Assets: listed for each specific flavour in the Service Flavours section.

Included Non-CIS Assets: listed for each specific flavour in the Service Flavours section.

Reporting: Manually generated, no automated 24/7 monitoring of the Service status/availability is feasible.

Configuration Changes:

Major – Defined as a significant change to the service, such as complete re-configuration of all or majority of key configuration items (change of the service baseline), primarily in order to prepare a service for a new mission. The standard change of the service baseline, costed as one complete change every two years. The schedule of Major Changes are agreed by both Provider and Customer in advance. The configuration baseline is made available to the customer through the Configuration Management Database.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability.

Configuration and maintenance of the backup capability included.

Maintenance:

Preventative Maintenance Inspections (PMI) – The PMI to the Service are conducted at support Level 3 (L3) and in coordination with Customer to take into account the impact on operational availability and requirements, as a standard, along with configuration changes schedules taking into account manufacturer's instructions on maintenance, or otherwise defined technical maintenance standards;

Corrective Maintenance Inspections (CMI) – CMI is undertaken by Provider in the event of Service asset failure, at support Level 3 (L3) and in accordance with the Customers' requirements as described in the service provisioning agreement. This includes replacement of non-reparable equipment, where applicable under NATO financial rules and regulations.

Maintenance includes regular sustainment of used applications and related licenses.

Shipment and transportation: Service assets will be provided at Customer's disposition at any of customer's permanent locations. Full shipping between the repair- and peacetime location is included.

Documentation: Customer will be provided with required technical documentation, as specified in the service provisioning agreement.

Spare parts: Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the factory state. Provider holds sufficient spares needed for Agency scheduled maintenance and anticipated incident resolution at the level to meet the service KPIs. Local users hold L1 spare parts in accordance with recommended

spare part list provided in the specifications for each system. Local users are responsible to request replenishments through Provider's Material Request Procedure.

Security Accreditation Documentation: Customer will receive prepared documentation required for the Security Accreditation.

Signal Support Group Cyber Defence Toolkit (SSG CDT) (SEC021):

Available as an option to specific flavours, as specified in the Service Flavours section. The feature supports a Deployed Network Operations Centre (DNOC) of a JFC Commander by providing a single deployable Cyber Defence Toolkit (SSG CD Kit) for monitoring the NU domain against intrusion.

Customer personnel operate the SSG CD Kit from the DNOC by adhering to all relevant NATO cyber defence related policies and processes. In the event that the cyber service is impacting the delivery of services to the user community, the provider will inform the customer and the service will be terminated immediately.

The SSG CDT feature entails:

- L3 engineering support;
- Microsoft standard software support to successfully detect malicious traffic, email attachments, SQL injection attacks, denial of service attacks, and other cyber threats; and
- Provision of the following security services: Cyber Security Incident Management Service (SEC006), Cyber Security Monitoring Service (SEC007), Cyber Security OPCEN Helpdesk Service (SEC008), Cyber Security Outreach Service (SEC009), Cyber Security Information Sharing Service (SEC010), Gateway Security Service (SEC011), and CIS Protection Support Service (SEC012).

There are the following assets included in this feature:

- CIS Assets: DNOC SIEM Server, Sensor Workstations, Eclypt Hard Drive (HDD), Eclypt External Hard Drive (HDD), Eclypt Hard Drive (HDD) Management, VPN/Firewall, VPN Concentrator/Firewall, and Network Taps (Datakom);
- Non-CIS Assets: General Purpose (GP) Tents, Environmental Control Unit (ECU), UPS, Racks, Power Strips.

Additional Options: listed for each specific flavour in the Service Flavours section.

Service Flavours: The flavours of the Service are designed with different capabilities to effectively meet all operational scenarios. Each flavour includes additional options to enable full adaptation of the Service to the operational requirements. Options are to be requested by the customer through the annual submission of the requirements changes, in accordance within the established and/or agreed requirements establishment and budgeting process. Any in-year change of options shall be dealt with in accordance with the procedures agreed within the service provisioning agreement. Costing of options is conducted on per request basis.

The flavours of the Service are:

Firefly (INF047) – is a 3 domain system integrated into transit cases, meets NRF requirement for low intensity operations, FMN compliant, can operate self-sustained without reach-back to the data center, provides standard user services and

capable of hosting a limited set of FAS applications (to be specified in the SLA). Each DPoP standard configuration is 1x Core Node, 2x RNM-A and 2x RNM-B.

Core Node and RNM-A support up to 30 users per domain. RNM-B only provide NIP access and do not provide user access. Interconnects using X-Band SATCOM, digital line of sight, military landline. The service is provided with non CIS assets; tents, ECU, UPS and manual handling equipment to enable operation in harsh environments between -32° and +49° Celsius.

The Service provisions the user equipment for 30 users and can be augmented by additional RNM-A (INF045) the STK (INF019-1) and DCEP Services (INF020) to bring it up to 270 users.

DragonFly (INF008) – a 3 domain system integrated into transit cases, full FMN and NRF compliant. Can operate self-sustained without reach-back to the data centre, provides standard user services and can host full set of FAS applications, supports up to 192 users per domain. Interconnects using X-Band SATCOM, digital line of sight, military or commercial landline. The service is provided with non CIS assets; tents, BC protection, and ECU, UPS and manual handling equipment to enable operation in harsh environments between -30° and +49° Celsius. The Service provisions the user equipment for 30 users and can be augmented by the DCEP Service (INF020) to bring it up to 192 users.

Communications Gateway Shelters (CGS) (INF010) – a 3 domain, shelter based system, that can operate self-sustained without reach-back to the data centre, provides standard user services and capable of hosting full set of FAS applications. It supports up to 250 users per domain. Interconnects using X-Band SATCOM (INF037), High Capacity Digital Line Of Sight (INF026), and military or commercial landline. The Service is provided with non-CIS assets, such as: shelters (CIS, crypto maintenance and system administration), ECU, UPS, and generators to enable operation in harsh environments between -30° and +49° Celsius. The CGS Shelter is transportable on any transportation equipped with TWIST-locks for 20-ft ISO Containers, including road, rail, cargo ship, and cargo aircraft means of transportation. The Service provisions the user equipment for 30 users and can be augmented by the DCEP Service (INF020) to bring it up to 250 users.

Limited Interim NRF CIS – Expansion (LINC-E) (INF009) – a 3 domain system integrated into transit cases, meets NRF requirement for low intensity operations but not FMN compliant as an interconnection node (no INM), can operate self-sustained without reach-back to the data centre, provides standard user services and capable of hosting a limited set of FAS applications (to be specified in the SLA), supports up to 126 users per domain. Interconnects using X-Band SATCOM, digital line of sight or military landline. The Service is provided with non-CIS assets: light cargo vehicles, tents, ECU, UPS, and generators to enable operation in harsh environments between -30° and +49° Celsius. The Service provisions the user equipment for 30 users that can be augmented by the DCEP Service (INF020) to bring it up to 126 users.

In-Theatre Mobile CIS Detachment (IMCD) (INF017) – a 3 domain system integrated into transit cases capable of supporting low intensity operations, does not meet the

requirements of NRF (not C130/C160 RORO) and not FMN compliant as an interconnection node, can operate self-sustained without reach-back to the data centre, provides only standard user services, and supports up to 40 users per domain. Interconnects using X-Band SATCOM, digital line of sight, or military landline. The service includes non-CIS assets: tents, ECU, UPS, and generators to enable operation in harsh environments between -30° and +49° Celsius. This Service provisions the user equipment for 30 users that can be augmented by the DCEP Service (INF020) to bring it up to 40 users.

Amphibious Command Platform (ACP) (INF061) – a 3 domain system integrated into transit cases, meets the requirement for a Joint Task Force (JTF) deployed on-board a NATO flag ship in support of NRF or a Maritime heavy operation, can operate self-sustained without reach-back to the data centre, provides standard user services and capable of hosting a limited set of FAS applications, supports up to 110 users per domain. Interconnects using SATCOM provided by the hosting vessel. Dependent on the hosting vessel to provide 18 KW of electric power and sufficient cooling. Provisioned with the user equipment for 110 users.

Mini Point of Presence (Mini-PoP) (INF018) – a 2 domain system integrated into transit cases capable of supporting low intensity operations, dependent on reach-back to data centre for services, provides only standard user services, not FMN compliant, and supports up to 12 users. Interconnects using X-Band SATCOM, digital line of sight, or military landline. The Service non-CIS support is limited to the UPS. The Service provisions the user equipment for 12 users that cannot be augmented.

Theatre Liaison Kit/ In-Theatre Liaison Kit/ Small Team Kit (TLK/ILK/STK) (INF019) – a 2 domain system integrated into transport cases capable of supporting low intensity operations, dependent on reach-back to data centre for services, cannot operate self-sustained, provides only standard user services, not FMN compliant. The system operates in one of three modes. BGAN, military SATCOM or terrestrial mode of operation. BGAN can operate up to 4 devices concurrently across the domains. The military SATCOM and terrestrial operation modes can operate up to 10 devices concurrently, which is a maximum of up to 6 laptops and 4 IP phones across the domains. The Service does not include any non-CIS assets. It provisions the user equipment for a maximum of 10 physical devices that cannot be augmented.

DCIS – Remote Network Module (RNM) (INF045)

The Remote Network Modules enable connection of nationally owned Deployable Communication and Information Systems (DCIS) to NATO DCIS in order to maintain and exercise Command and Control (C2) in accordance with the operational requirements of the NATO Readiness Forces (NRF). The users connected to the national DCIS will benefit from services hosted remotely on the NATO DCIS with neither DCIS system having to deploy. By adding a User Access Module (UAM), the RNM has the functionality to host up to 20 directly connected users per information security domain who will receive services provided from the remote NATO DPOP. This function does not require the connection of national DCIS system. The RNM can connect to the NATO DCIS described under INF035 (INF008 and INF009) in the NCI

Agency Costed Customer Service Catalogue (CCSC). All services hosted on the NATO DCIS system are available for extension to and through the Remote Network

Feature/Option	FireFly	DragonFly	CGS	LINC-E	IMCD	ACP	RNM	Mini-PoP	TLK/ILK
General									
Maintenance and repair of non-CIS equipment and supply of L1 – L3 system spare parts and consumables, including also crypto spares, is included within the funding specified in the service provisioning agreement.	X	X	X	X	X	X	X	X	X
Maintenance/ sustainment/ replacement of UPSs	X	X	X	X	X	X	X	X	
Included NCI Agency Services									
NDW001 NATO Digital Workplace Service(Low Side)	X	X	X	X	X	X		X	X
NDW002 NATO Digital Wokrplace Service(High Side)	X	X	X	X	X	X		X	X
NDW003 Personal Workspace – Managed Device Service	X	X	X	X	X	X		X	X
WPS009 Voice Collaboration Service	X	X	X	X	X	X		X	X
WPS010 Video (VTC) Collaboration Service	X	X	X	X	X	X		X	
WPS012 E-Mail Service	X	X	X	X	X	X		X	X
INF003 Enterprise Internet Access Service	X	X	X	X	X	X		X	X
INF007 Infrastructure Storage Service	X	X	X	X	X	X			
WPS007 Print/ Scan/ Copy Service	X	X	X	X	X	X		X	X
INF016 Infrastructure Backup/Archive Service	X	X	X	X		X			
INF001 LAN Service	X	X	X	X	X	X		X	
INF002 NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service (only WAN Infrastructure Assets feature)		X							
INF005 Infrastructure Integration Service	X	X	X	X	X	X		X	
PLT001 Information Sharing and Collaboration Platform Services	X	X	X	X	X	X			
PLT003 Web Hosting Service	X	X	X	X	X	X			
PLT006 Database Platform Service	X	X	X	X	X	X			
WPS014 Secure Voice Service	X	X	X	X	X	X		X	
APP029 Military Message Handling Application Service	X	X	X	X	X	X			
Included CIS Assets									
µCOM	X	X	X	X	X	X			
IEG-B and IEG-C	X	X	X	X		X			
Break Our Boxes (BOB)	X	X	X	X	X	X		X	
MS Core	X	X	X	X	X	X		X	X
NU Core	X	X	X	X	X	X		X	X
NS Core	X	X	X	X	X	X		X	X
SATCOM Modems						X			
SATCOM terminals (DART and BBSST or BGAN).								X	X
Crypto Assets	X	X	X	X	X	X		X	X
Helpdesk Assets	X	X	X						
NAS	X	X	X	X		X			

Feature/Option	FireFly	DragonFly	CGS	LINC-E	IMCD	ACP	RNM	Mini-PoP	TLK/ILK
μISM	X	X	X	X	X	X			
Intra Nodal Distribution System (INDS)		X							
Service Access Points (SAP)									
Cyber Defense	X	X	X	X	X	X		X	X
Element Network Manager (ENM)		X							
Integrated Network Management System (INMS)		X							
Interface to Nations Module (INM)	X	X							
Remote Network Module (RNM)	X	X	X	X	X	X			
Included Non-CIS Assets									
Power Generator			X		X				
Environmental Control Unit	X	X	X	X	X				
Power Generator Set (PGS)				X*					
Cargo Transport Cases	X	X*	X*	X*	X*	X*	X*	X*	X*
Racks						X*			
Uninterrupted Power Supply (UPS)	X	X	X	X*	X*	X*	X	X	X
Transit case	X	X	X	X	X	X	X	X	
Tent (with Furniture)	X	X	X	X	X				
Biological Chemical Tent and Filters	X	X							
Manual Handling Equipment		X							
Available Options									
Additional Baseline Changes	X	X	X	X	X	X	X	X	X
Increase in Service Availability	X	X	X	X	X	X	X	X	X
Change to Service Restoration Period	X	X	X	X	X	X	X	X	X
Additional Domain Change								X	
Functional Area Services (FASs to be specified within the service provisioning agreement)	X	X	X	X					
ISO standard transportation containers		X		X					
Additional Prerequisites									
Operators and maintainers completed the Agency approved training.	X	X	X	X	X	X	X	X	X
Customer ensures the provision of secure facility to enable operation	X	X	X	X	X		X	X	X
Domain Availability									
Single domain									
2 Simultaneous Domains							X	X	X
3 Simultaneous Domains	X	X	X	X	X	X	X		

* Number of assets depending on the chosen options

** Number of assets depending on the requested operational configuration

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites: In general, the Service requires Qualified Operators provided by the customer and are trained to the standard specified by the Agency. Specific prerequisites, where applicable, are specified in the Service Flavours section.

Underlying Services: OTH004, SME005, TRA002

Standard Service Support Levels:

Service Availability Target: The service is costed with an availability target of 95% excluding scheduled downtime for maintenance. This is based on the assumption that the system may be in remote locations without local Agency support.

Service Restoration Period: The service is costed with a restoration of 80% of all incidents within 3 calendar weeks. This is based on the assumption that the system may be in remote locations without local Agency support.

Service Cost / Price: The unit of measure for each of the Service Flavours is Per System. Price details available in the Costed Customer Service Catalogue.

INF036 DCIS – Deployable SATCOM Service

Service ID: INF036

Service Name: DCIS – Deployable SATCOM Service

Portfolio Group: Infrastructure Services

Service Description: The Service provides a Deployable CIS to deployed commands of the NATO Allied Response Force (ARF) enabling them to:

- Communicate between deployed NATO command units.
- Access the NATO strategic communications infrastructure and the Bilateral Strategic Command (Bi-SC) Automated Information Service (AIS).
- Communicate with mission partnering Nations and non-governmental organisations.

Value Proposition: This service is aligned to the NATO Digital Backbone concept and supports multi Domain Operations at the strategic centre and the tactical edge depending on the service delivery point. The Service extends C2 ability globally, thus enabling Operational Commanders to execute Allied Operations and Missions worldwide.

- **Modularity:** Discrete elements may be combined as required for the deployment scenario and equipment can be interchanged or upgraded without having to replace large bespoke modules.
- **Scalability:** configurable from small C2 deployments through to a large deployment.
- **Deployability:** Deployable SATCOM is a solution for rail, sea, and tactical air transport. It may be fully operational in theatre within 72 hours of arrival on site, with a subset of priority services to be available within 48 hours. Equipment is integrated into either ruggedized outdoor and indoor transit cases or in shelters that can be loaded onto military transportation vehicles.
- **Sustainability:** comprises Commercial off the Shelf (COTS) software that are interchangeable, upgradable, reconfigurable and replaceable.
- **Interoperability:** provides interoperability with NATO Headquarters (HQ), Nations forces, Governments and Non-Government Organisations through standards-based interfaces and conformance to the NATO Federated Mission Network Interoperability Profile.
- **Service Management:** The customer will have direct access to the Agency Service Management team throughout the period of delivery as described in the OTH004 Service description.
- **Reporting:** The customer is provided with access to the NCIA ITSM Toolset that enables monitoring of the service status and service availability. Additionally, the monthly service activity reports are provided.

Service Features:

The NCI Agency services in deployed environment:

- SATCOM (INF012);
- Managed Devices Service - Laptop (WPS001);

The above listed services correspond with standard NCI Agency services, as described in respective service definitions. However, due to deployable nature of the entire Deployable SATCOM Service, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences are to be elaborated in detail within the respective service provisioning agreement. Delivery cost of these services differs from the standard service rates, and it is included within Deployable SATCOM Service delivery cost.

CIS Assets: listed for each specific flavour in the Service Flavours section.

Non-CIS Assets: listed for each specific flavour in the Service Flavours section.

Configuration Changes:

Major – Defined as a significant change to the service with the replacement of components that have reached end of life. The schedule of Major Changes is agreed by both Provider and Customer in advance and is managed and maintained by both parties. The new configuration will be made available to the customer.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability.

Maintenance:

Defined and provided by the NCIA as Preventative Maintenance Inspections (PMI) and Corrective Maintenance Inspections (CMI) on all Service assets.

- PMI – The PMI to the Service are conducted at support Level 3 (L3), as a standard, along with configuration changes schedules taking into account manufacturer's instructions on maintenance, or otherwise defined technical maintenance standards;
- CMI – In the event of Service asset failure, Provider undertakes CMI at support Level 3 (L3) and in accordance with the Customers' requirements as described in the service provisioning agreement.

Maintenance includes regular sustainment of used applications and related licenses.

Shipment and transportation: Service assets will be provided at Customer's disposition at any of customer's permanent locations. Full shipping between the repair- and peacetime location is included.

Spare parts: Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the factory state. Provider holds L1 and L2 spares needed for PMIs, CMIs, and uplifts. All L3 spares are held by Provider. Local users hold L1 and L2 spare parts in accordance with recommended spare part list provided in the specifications for each system. Local users are responsible to request replenishments through Provider's Material Request Procedure.

Additional Options: Additional Baseline Changes, Increase in Service Availability, and Change to Service Restoration Period.

Costing of options is conducted on a per request basis. Options are to be requested along with any possible additional requirements for Major Changes. Any in-year change of options shall be dealt with in accordance with procedures agreed within the service provisioning agreement.

Service Flavours:

TSGT (INF021) – the Generation 3 Transportable Satellite Ground Terminal (TSGT) and Upgraded generation 2 terminals (UTSGT) are vehicle mounted Satellite transmission systems that are designed for high capacity links utilizing the military X-Band space segment. Each terminal is capable of providing up to six 8-Mbit satellite bandwidth carriers. Both types of terminal have a 4.6 m antenna and redundant 750 W amplifiers, and the TSGT has additional functionality with an addition of a rapidly deployable 2.4 m pop-up antenna with redundant 250 W amplifiers enabling the terminal to establish simultaneous communications over two different satellites. Each terminal is operated by the deployed CIS crew and can be remotely managed by NCI Agency utilizing an out of band management system.

The systems can be interconnected over Fiber optic Ethernet to Dragonfly, CGS, LINC-E, IMCD, or Mini PoP flavours of DCIS Nodes Service. The service is provided with non-CIS assets enabling operation in harsh environments between -30° and +49° Celsius.

Available sub-flavours:

- **TSGT3G – T1 Variant:** may use optionally the 4.6 meter or the 2.4 meter pop-up antenna, Dual Satellite Operation. Maintenance includes the re-integration of NSPA-maintained PGS into SATCOM systems by NCIA;
- **TSGT3G – T2 Variant:** equipped with the 2.4 meter pop-up antenna single satellite operation. Maintenance includes the re-integration of NSPA-maintained PGS into SATCOM systems by NCIA;
- **Upgraded TSGT (UTSGT):** 4.6m antenna single satellite operation.

Included CIS Assets:

- Antenna ;
- Redundant Solid state power amplifier (SSPA)

- Redundant Low Noise Amplifiers (LNA)
- PSK & EMS modems (quantities can be defined by the customer)
- Management system enabling remote operation and service monitoring.
- I.P. Baseband module
- System Engineer PC/ Laptop.

Included non-CIS Assets:

- Power Generation System (PGS; UTSGT only);
- Antenna heaters
- 3rd Generation TSGT Generator;
- Antenna Trailer TSGT 2nd generation;
- Shelters with AIRCO System (ECU);
- UPS;
- BC Protection System.

Number of non-CIS assets depends on the specific configuration for each deployment.

DSGT (INF022) – the Deployable Satellite Ground Terminal (DSGT) is a modular terminal in transit cases that can be transported by light commercial vehicles, designed for medium capacity links utilizing the military X-Band space segment. Each terminal has a 2.4 m 200 W single amplifier that is capable of providing up to four carriers with a total throughput of up to 12Mbit. Each terminal is operated by the CIS crew deployed and there is currently no remote management capability. The system can be interconnected over Fiber optic Ethernet to Dragonfly, CGS, LINC-E, IMCD or Mini Pop flavours of DCIS nodes. The service non-cis support is limited to the UPS.

Available sub-flavours:

- **INF022-2: Dual-band DSGT:** consists of a 2.4 meter X-band and Ka band antenna and featuring an 200 watt power amplifier and a maximum duplex data link capacity of 8Mbit/sec on global beam

Included CIS Assets:

- 1st Generation Deployable Transportable Satellite Ground Terminal (1st Generation DSGT) / 2nd Generation Deployable Transportable Satellite Ground Terminal (2nd Generation DSGT);
- Dual-band Deployable Transportable Satellite Ground Terminal
- System Engineer PC/Laptops.

Included non-CIS Assets: UPS and Transit Cases.

FAST(INF032) – Fly Away SATCOM Terminal (FAST) are small modular terminals in hardened cases rapidly deployable and transportable light commercial vehicles, designed for low capacity links utilizing the military X-Band and commercial Ka Band space segment. Each terminal has a 1.2 m 125W single amplifier that is capable of providing a single carrier with a

maximum throughput of up to 2 Mbit. The deployed CIS crew operates each terminal, with no remote management capability. The system can be interconnected over Fibre optic Ethernet to Mini-PoP or ILK/TLK flavours of Deployable CIS Nodes Service.

Available sub-flavours:

- **INF032-1 TP120 SATCOM** (Military X-band & Commercial Ka-band)
- **INF032-2 CCT200 SATCOM** (Military X-band only)

Included CIS Assets:

- Fly-Away SATCOM Terminal (FAST)
- Antenna 1.2M;
- Antenna Tracking Controller;
- Ruggedized Laptop.

Included non-CIS Assets: UPS, Tent, Cargo Vehicle Rough Terrain (CVRT type SHERPA), Trailer, and PGS.

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

User provided Qualified Operators

Underlying Services: OTH004, SME005, TRA002

Standard Service Support Levels:

Service Availability Target: In accordance with the stipulations of the service provisioning agreement and based on the Customer requirements.

Service Restoration Period: In accordance with the stipulations of the service provisioning agreement.

Available NCI Academy Training not covered by service cost:

A0045	NATO Ku-Band VSAT Operator

INF021:

A0043	NATO X-Band TSGT G3 Operator Level 1
A0047	NATO X-Band UTSGT Operator
A0052	NATO X-Band TSGT G3 Operator Level 2

INF022:

A0040	NATO X-Band DSGT Operator Level 1

A0041	NATO X-Band DSGT Operator Level 2
A0903	NATO CALI DSGT Operator

INF032:

Ref TBC	FAST TP120 Operator
N/A	CCT200 Operator (<i>provided by Luxembourg Army</i>)

Service Cost / Price: The unit of measure for the Service is Per System. Price details available in the Service Rates document.

INF037 DCIS – Deployable Radio Transmission Service

Service ID: INF037

Service Name: DCIS – Deployable Radio Transmission Service

Portfolio Group: Infrastructure Services

Service Description: The Service provides a directional transmission service and secure voice and data transfer capability based on the HF/VHF radio communication systems to deployed commands of the NATO high readiness Response Force (NRF) enabling them to communicate between deployed NATO command units and down to the tactical user.

Value Proposition:

Transportable via road, rail, sea, and tactical air transport, the systems may be operational in theatre within 4 hours of arrival on site. The customer is provided with access to the NCIA ITSM Toolset that enables monitoring of the service status and service availability.

Service Management : The customer will have direct access to the Agency Service Management team throughout the period of delivery as described in the OTH004 Service description.

Service Features:

Included NCI Agency Services: listed for each specific flavour in the Service Flavour section.

Included NCI Agency Services correspond with standard NCI Agency services, as described in respective service definitions. However, due to deployable nature of the entire Deployable Radio Communications Service, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences are to be elaborated in detail within the respective service provisioning agreement. Delivery cost of these services differs from the standard service rates, and it is entirely included within the Deployable Radio Transmission Service delivery cost.

Included CIS Assets: listed for each specific flavour in the Service Flavour section.

Included Non-CIS Assets: listed for each specific flavour in the Service Flavour section.

Reporting: Manually generated, no 24/7 monitoring of the Service status/availability feasible.

Configuration Changes:

Major – Defined as a significant change to the service, such as complete re-configuration of all or majority of key configuration items (change of the service baseline), primarily in order to prepare a service for a new mission.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted

continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability.

Maintenance:

Preventative Maintenance Inspections (PMI) – The PMI to the Service are conducted at support Level 3 (L3) and in coordination with Customer to take into account the impact on operational availability and requirements, as a standard, along with configuration changes schedules taking into account manufacturer's instructions on maintenance, or otherwise defined technical maintenance standards;

Corrective Maintenance Inspections (CMI) – CMI is undertaken by Provider at support Level 3 (L3) in the event of Service asset failure, in accordance with the Customers' requirements as described in the service provisioning agreement. This includes replacement of non-reparable equipment, where applicable under NATO financial rules and regulations.

Shipment and transportation: Service assets will be provided at Customer's disposition at any of customer's permanent locations. Full shipping between the repair- and peacetime location is included.

Documentation: Customer will be provided with required technical documentation, as specified in the service provisioning agreement.

Spare parts: Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the factory state. Provider holds L1 and L2 spares needed for PMIs, CMIs, and uplifts. All L3 spares are held by Provider. Local users hold L1 and L2 spare parts in accordance with recommended spare part list provided in the specifications for each system. Local users are responsible to request replenishments through Provider's Material Request Procedure.

Security Accreditation Documentation: Customer will receive prepared documentation required for the Security Accreditation.

Additional Options: Additional Baseline Changes, Increase in Service Availability, Change to Service Restoration Period.

Customer requests for in-year Major Changes, in addition to the service provisioning agreement agreed Major Changes, shall be dealt with in accordance with procedures agreed within the service provisioning agreement.

Service Flavours:

DCIS HF (INF024-1) – the deployable High Frequency Radio system enabling secure voice and data chat services between the users in the field and the commands in the 3 – 30MHz range. The system is built into transit cases (t-cases) that can be deployed in a tent or building of opportunity. No interconnection to DCIS Nodes available.

Included CIS Assets: HF Radio Systems; with telescopic Clark mast and antenna and user laptop.

Included non-CIS Assets: Transit case.

DCIS HF (INF024-2) – the deployable High Frequency Radio system enabling secure voice and data chat services between the users in the field and the commands in the 3 – 30MHz range. The system is built into transit cases that can be operated from within the transportation vehicle or deployed in a tent or building of opportunity. No interconnection to DCIS Nodes available. The service includes supporting non-CIS assets to enable operation in harsh environments between -30° and +49° Celsius.

Included CIS Assets: HF Radio Systems; with telescopic Clark mast and antenna and user laptop.

Included non-CIS Assets: Biological - Chemical (BC) Shelter; Uninterruptible Power Supply (UPS); Power Assembly; Generators; Lifting Device.

Maintenance includes the re-integration of NSPA-maintained PGS into SATCOM systems by NCIA.

DLOS (INF025) – the deployable Line Of Sight is capable of establishing a Digital Transmission link utilising I.P. over Ethernet at a data rate of up to 800Mbit per second using adaptive modulation up to a distance of 50km. The system is assembled into transit cases operable from within the transportation vehicle or deployed in a tent or building of opportunity. Possible interconnection over Fibre optic Ethernet to INF035 Services. Non-CIS assets included to enable operation in harsh environments between -30° and +49° Celsius. Each system consists of one BC protected shelter mounted on an all-terrain vehicle.

Included CIS Assets: UHF Radio, Fibre Optic System; Switch; Modem; F.O. Multiplexer; Mast; Self-Aligning Antenna.

Included non-CIS Assets: BC-Shelter; ECU; UPS; Lifting device.

Available on: N/A

Service Prerequisites:

User provided Qualified Operators

Underlying Services: OTH004, SME005, TRA002

Standard Service Support Levels:

Service Availability Target: In accordance with the stipulations of the service provisioning agreement and based on the Customer requirements.

Service Restoration Period: In accordance with the stipulations of the service provisioning agreement.

NCIA academy Trainings Available (INF025):

A00246	DLOS Operator/Technician

Service Cost / Price: The unit of measure for the Service is Per System. Price details available in the Service Rates Document.

INF038 DCIS – Deployable Nodes Anchor Service

Service ID: INF038

Service Name: DCIS – Deployable Nodes Anchor Service (Mission Anchor Function – MAF)

Service Type: Enabling Service

Portfolio Group: Infrastructure Services

Service Description: The Service enables the operational user to prepare the Deployable CIS Nodes in garrison and keep them at high readiness to deploy, as well as to interconnect to NATO General-Purpose Communications System (NGCS) when deployed. With the DCIS Nodes installed in garrison in the Mission Preparation Centre (MPC; a.k.a. PoP Replication Centre, PRC), they are interconnected to the Deployable Operational Gateway (DOG) from where they will synchronize the services, replicate all user data, and interconnect to deployed DCIS Nodes.¹

Service Status: Active

Value Proposition:

The service enables the interconnection of INF035 services whilst in peace time location to any one of the prepared Mission Domains 24/7/365. The service enables the continuous replication of mission data and implementation of regular patch updates thus ensuring that the DCIS systems are ready to deploy at very short notice. The service provides the secure network connections and information exchange capabilities between DCIS, static and federated domain users.

This service, aligned with NATO Digital Backbone concept, is the very core of DCIS Multi Domain Operations, supporting warfighters from the strategic centre to the tactical edge.

The customer will have direct access to the Agency Service Management team for Deployable CIS and will be supported as described in the OTH004 Service Description.

The Service includes sufficient tools and test equipment to prepare the DCIS Nodes, Satellite Communication, and Radio Transmission assets for deployment and subsequent interconnection to NGCS.

Service Features:

Included NCI Agency Services: listed for each specific flavour in the Service Flavour section.

Included NCI Agency Services correspond with standard NCI Agency services, as described in respective service definitions. However, due to deployable nature of the assets interconnecting with Deployable Nodes Anchor Service, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences are to be elaborated

¹ Throughout this Service Description, all reference to Mission Secret (MS) network or domain is to be considered under the new Vigilance and Enhanced Vigilance Activities Mission Network (VeVA MN) SH/CYBER/J6/SPP/080/23-015016 – Implementation of VeVA MN – dated 16 Oct 2023

in detail within the respective service provisioning agreement. Delivery cost of these services differs from the standard service rates, and it is entirely included within the Deployable Nodes Anchor Service delivery cost.

Included CIS Assets: listed for each specific flavour in the Service Flavour section.

Included Non-CIS Assets: listed for each specific flavour in the Service Flavour section.

Obsolescence Management considerations have been included within INF038 Service Rates.

Reporting: This service is monitored 24/7 and availability reports will be provided.

Configuration Changes:

Major – Defined as a significant change to the service, such as complete re-configuration of all or majority of key configuration items (change of the service baseline), primarily in order to prepare a service for a new mission.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability.

Maintenance:

Preventative Maintenance Inspections (PMI) – The PMI to the Service are conducted in coordination with Customer to take into account the impact on operational availability and requirements, as a standard, along with configuration changes schedules taking into account manufacturer's instructions on maintenance, or otherwise defined technical maintenance standards;

Corrective Maintenance Inspections (CMI) – CMI is undertaken by Provider in the event of Service asset failure, in accordance with the Customers' requirements as described in the service provisioning agreement. This includes replacement of non-reparable network and information system hardware, the Service includes shipping to/from repair facility, and supply of Level 1 through Level 3 system spare parts and consumables. In support of the DCIS mission preparation, the Provider conducts overall management of all activities.

Routine maintenance within Deployable Anchor Nodes Service will be outsourced to industry partners wherever possible enabling NCIA resources to perform increased Change Management activities to support tailored mission requirements.

The Decentralization of INF038 spares will enable increased Incident Resolution in time of relevance.

Additional options: Additional Baseline Changes; Increase in Service Availability; Change to Service Restoration Period.

Service Flavours:

DOG (INF026) – the Deployable Operational Gateway Service (DOG) provides two anchor points for all NATO deployable forces that interface into the NATO General Purpose Communication Systems (NGCS) static CIS network as well as between NATO Secret (NS) and Mission Secret (MS) domains, or among different MS domains. Each of the DOG systems provides 4 (four) security domains (NS, NU, and 2X MS), with each domain providing the complete set of mission information exchange requirements to support the operational commands on deployment. The DOG is hosted in the two NCI Agency data centres and are interconnected with the Satellite Ground Stations (SGS) and Mission Information Room (MIR) that enables enterprise wide connectivity of users to the mission services.

Included NCI Agency services: LAN Service (INF001); NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service (INF002); Infrastructure Integration Service (INF005); Infrastructure Storage Service (INF007); Infrastructure Backup/Archive Service (INF016); Managed Devices Service for the system administrators (WPS001); E-Mail Service (WPS012); Print/ Scan/ Copy Service (WPS007); Voice Collaboration Service (WPS009); and Video (VTC) Collaboration Service (WPS010).

Maintenance is conducted at support Levels 1-3 (L1-L3), and it includes regular sustainment of used applications and related licenses.

Configuration and maintenance of the backup capability is included.

Available sub-flavours:

- None

Included CIS Elements:

- Terrestrial network connectivity into NGCS and the respective NS, MS and NU domains;
- Satellite Connectivity;
- BGAN network interconnectivity with Inmarsat ;
- X Band Satellite connectivity through the SGT terminal with each DOG able to provide connectivity for 12 deployed TSGTs;
- An IEG-C for cross-domain service flows;
- Cross-domain Service interfaces for Mail, Voice and VTC.

Included CIS Assets:

- Transmission and Network layer routing with redundancy;
- Distribution Layer Switches;
- Border Protection Firewalls;
- Voice Call Managers;
- VTC collaboration systems;
- Cross domain capability for mail and file transfers, low to high and between high side domains;
- Centralised Services for security patching for each domain;

- Crypto Equipment.

MPC/PRC (INF027) – the Mission Preparation Centre or PoP Replication Centre (MPC or PRC) is an in-garrison capability to connect Deployable Nodes in the static domain to the deployed Mission Secret domains in order to enable the replication of user data and the update of services between the DOG and Deployable Nodes. The MPC/PRC capability is essential to support the operational requirement for 48 hours or 5-days notice to move. For MPC/PRC on short NTM, e.g. assigned to mission in stand-by, COI enabling and COI services are installed and operational, supporting the generic C2 service requirements of the leading HQ that the specific PoP will support upon deployment. Additionally, all applicable IA tools and processes are set as active. In support of the DCIS mission preparation, the Provider conducts overall management of all services, to include enabling the distribution of Mission-specific configuration updates, system patches, security patches and updates, and also supports on-the-job training of Customer personnel.

Included NCI Agency services: Gateway Security Service (SEC011); Managed Device Service (WPS001); and Print/ Scan/ Copy Service (WPS007).

Maintenance is conducted at support Level 3 (L3).

Spare parts: This flavour of the Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the factory state. Provider holds L1 and L2 spares needed for PMIs, CMIs, and uplifts. All L3 spares are held by Provider. Local users hold L1 and L2 spare parts in accordance with recommended spare part list provided in the specifications for each system. Local users are responsible to request replenishments through Provider's Material Request Procedure.

Included CIS Assets:

- Distribution Layer Switches
- NGCS Access interconnects

Prerequisite: INF038 DCIS – Deployable Nodes Anchor Service (DOG flavour). Locations hosting systems require appropriate security certification for storage and use of cryptographic equipment and key material, connection to the NGCS Protected Core Segment which allows interconnection with the NGCS Gateways, deployed nodes and the NCI Agency Network Control Centre (within ESOC), and sufficient test equipment to simulate other Nations' networks.

Available on:

NATO Unclassified Domain
NATO Secret Domain
Multiple Mission Secret Domains

Service Prerequisites: None, unless specified in the Service Flavours section for specific flavours.

Underlying Services: INF046, OTH004, SME005



Standard Service Support Levels:

Service Availability Target: In accordance with the stipulations of the service provisioning agreement and based on the Customer requirements.

Service Restoration Period: In accordance with the stipulations of the service provisioning agreement.

Service Cost / Price: The unit of measure for the Service is Per System. Price details available in the Service Rates document.

INF040 Ultra High Frequency (UHF) Tactical Satellite (TACSAT) Radio Services

Service ID: INF040

Service Name: UHF TACSAT Services

Portfolio Group: Infrastructure Services

Service Description: The NATO Ultra High Frequency (UHF) Tactical Satellite (TACSAT) Radio Services provide secure low data rate communication links to the tactical edge in all battle-space environments, in both the back-pack and vehicle-mounted configuration.

The TACSAT terminals come equipped with a U.S Type 1 Control Cryptographic Item (CCI) radio and associated ancillaries required to communicate in both secure voice and secure data at all NATO classifications. The NATO terminals are capable of operating in Single Carrier Per Channel (SCPC), Demand Assigned Multiple Access (DAMA) and Integrated Waveform (IW), with data rates of up to 64Kb/s.

The current NATO TACSAT is the Harris AN/PRC 117F.

Please note that this service does not cover the TACSAT network subsystem, the NATO UHF Control Capability (NUCC); this is covered under the INF012 SATCOM Service.

The customer will have direct access to the Agency Service Management team for Deployable CIS and will be supported as described in the OTH004 Service Description.

Value Proposition: NATO's UHF network is a set of complex systems that provides NATO forces with access to a secure tactical radio SATCOM network across NATO's Area of Responsibility (AOR). The UHF SATCOM capabilities are used to support NATO Land, Sea and Air operations, providing secure voice and data capabilities.

The UHF TACSAT network and terminal requirements are based on the need to support the Core mission requirements associated with Capability Level 1 and 2, which represent the MJO 1, SJO 2, SJO 5 and SJO 6 missions. In addition, any Allied Operations and Missions (AOM), standing air and maritime requirements as well as training requirements have been taken into consideration.

Service Features: Point to Point and Point to Multi Point Tactical communications consisting of voice, email, chat and local FTP.

Service Request: The ACO-endorsed technical report 2017/NSP011502/01 defines the quantity and allocation plan of the current and future NATO TACSAT terminals. Requests for TACSAT assets outside of the technical report must be pre-approved by ACO J6 via formal communication before the assets will be released by NCIA through ITSM and EBA.

Service Flavours: The UHF TACSAT Radios capability consist of two variants:

- On-The-Pause (OTP), back-pack portable configuration and On-The-Move (OTM), vehicle- or mobile-mounted configuration
- Static installation, consisting of the additional equipment (Matrix switch, antennas, amplifiers, cables etc) installed at static sites

Available on:

Standalone

Service Prerequisites:

To be able to utilise the TACSAT SATCOM service a Satellite Access Authorisation (SAA) must be in place through the SATCOM Service (INF012).

Underlying Services: OTH004, SME005

Standard Service Support Levels:

Service Availability Target: 95.0 %

Service Restoration:

	Restoration Time
Level 0 Related (User)	<2 hrs
Level 1 Related (CSU)	2-24 hrs
Level 2 Related (CSSC)	1-10 working days
Level 3 Related (Vendor)	>90 working days

Available NCI Academy Training not covered by service cost:

A0037	UHF TACSAT Basic
A0038	UHF TACSAT Applications & Data Base Manager

Service Cost / Price: The unit of measure for the Service is Per Device. For price details please see the Service Rates Document.

INF041 CRC System Interface (CSI) Local Support Service

This service is moved under the APP087 CRC System Interface (CSI) Application Service as one of its service flavours. The service ID INF041 will be retained for financial tracking purposes (please see APP087 for further clarification).

INF042 ADatP-3 Gateway Service

Service ID: INF042

Service Name: ADatP-3 Gateway Service

Portfolio Group: Application Services

Service Description: Currently NATO CAOCs use ICC as their primary Air C2 system while subordinate ARS are gradually moving to ACCS. This requires exchange of message-based information products, ADatP-3, between ACCS and ICC. ACCS uses STANAG 4406 as messaging protocol while ICC uses SMTP. This requires translation between STANAG 4406 and SMTP messaging protocols, which is provided by the ACCS ADatP-3 Gateway (GWY).

Value proposition: The service enables the exchange of formatted (AdatP-3 messages) between ACCS and ICC.

Service Features: The ACCS SMTP gateway consists of two COTS products, XOMail server for STANAG 4406 and Exchange server for SMTP translation. The GWY is currently available and working but it is considered as a single point of failure for its centralized architecture

Service Flavours:

None

Available on:

NATO Secret

NATO Classified

Service prerequisites:

APP049 (ICC)

APP050 (ACCS)

SEC022 (ALF-SFP)

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)

Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number:

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request the INF042 service please complete the Customer Request Form and contact NCI Agency Demand Management.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions between NCIA and SHAPE on an annual basis via AMDC2 ISS POW.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
INF042A	ADatP-3 and Air Traffic Management (ATM) Gateway Service	AdatP-3 Gateway	1
INF042B	ADatP-3 and Air Traffic Management (ATM) Gateway Service	ATM Gateway	1

KPIs: No service availability monitoring KPIs are defined.

In case an SLA is established for AdatP-3 Gateway support the standard NCI Agency service support KPIs (response and restoration times) apply unless otherwise negotiated.

INF043 NATO Partner Network Service

Service ID: INF043

Service Name: NATO Partner Network Service

Portfolio Group: Infrastructure Services

Service Description: The NATO Partner Network Service provides Secured NATO client devices that allow collaboration among NATO and Military Partnerships entities to cooperate and share documentation up to a Security level of NATO Unclassified.

The Client device is loaded with the office automation software (MS Office Professional Suite and Adobe Acrobat Reader), Windows operating system, and NATO recommended security tools.

The service can also provide Remote connectivity via NATO Enterprise Managed Mobility Service.

Value proposition: The NATO Partner Network Service is a bundle of customer facing services (Managed Device, Enterprise Identity Access Management Service, E-mail Service, Printer Service and Information sharing and collaboration Platform Service, Infrastructure and Security Services). This allows the production of documentation, presentations etc., in support to the business processes of the NPN users located in SHAPE campus; the service also allows collaboration with external entities via email capability and can be extended to external entities via Remote connectivity capabilities.

Service Features: The Service includes a fully NATO managed end user device and a possibility to collaborate within the NPN Domain via a customized Web Content Management Portal. The NPN Partner Network Collaboration Service also includes an E-Mail capability.

Service Flavours:

Portable Client Device (Laptop) – provides a Laptop device that needs to be connected to a wired or wireless network. A power supply and an external mouse are also included in the package. Access to the NPN network is provided via a secure VPN solution.

Static Solution – provides a laptop device connected to an internal wired network. This solution features a docking station, a media converter, an external monitor, a keyboard, and a mouse.

Available on:

NATO Partner Network Unclassified

Service prerequisites:

This service encompasses a number of other catalogues services (INF, PLT, WPS, SEC).

Underlying Services: OTH001

Standard Service support levels:

Service Availability Target: 99.0% Availability

Service Restoration: The service delivered as P4.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is 1. The total of the service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate.

Please see Service Rates document for standard rates applicable to the service.

INF049 Air Traffic Management (ATM) Gateway (GW) Service

Service ID: INF049

Service Name: ATM Gateway Service

Portfolio Group: Infrastructure Services

Service Description: The ATM GW is a system that feeds any AirC2 system, with the flight plans provided by the various national Air Traffic Control (ATC) systems. This function is fundamental in order to create a credible and complete Recognised Air Picture (RAP) in the various ARSs where it is installed because it facilitates the correlation/recognition of the Air Breathing Threats (ABTs)

Value proposition: The service enables the exchange of flight plans and ATM Data between AirC2 systems and ATM/ ATC Centres.

Service Features: The ATMGW consists of a redundant HW server, operating a Oracle Linux OS, with an ATMGW Server and Client to receive and transmit Flightplan messages in different message formats (ICAO and ADEXP), to convert those messages in a different format and to receive and transmit these messages via different protocols (AFTN, AMHS, FMTP, FDE)

Service Flavours: The ATMGW Server/client configuration represent a singleton service in support of active ACCS sites

Available on:

NATO Secret

NATO Classified

Service prerequisites:

APP050 (ACCS) – (or non-ACCS system i.e. MASE)

SEC022 (ALF-SFP)

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)

Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number:

Belgium +32 65 44 3177
 Netherlands +31 70 374 3177
 Italy +39 081 721 3177
 Germany +49 282 4978 3177
 USA +1 757 747 3177
 For NATO HQ +32 (0)2 707 5858

Service Requests:

To request the INF049 service please complete the Customer Request Form and contact NCI Agency Demand Management.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions between NCIA and SHAPE on an annual basis via AMDC2 ISS POW.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
INF049	ADatP-3 and Air Traffic Management (ATM) Gateway Service	ATM Gateway	1

KPIs: No service availability monitoring KPIs are defined.

In case an SLA is established for ATM Gateway support the standard NCI Agency service support KPIs (response and restoration times) apply unless otherwise negotiated.

INF053 Internet Website Publishing and Protection Service

Service ID: INF053

Service Name: Internet Website Publishing and Protection Service

Portfolio Group: Infrastructure Services

Service Description: The Internet Website Publishing and Protection Service provides the cradle to grave management of the publication of NATO websites on the Internet. This includes the coordination required for the site to abide by the applicable NATO Security Directives, the issuing of NATO.INT DNS names, the provision of required SSL certificates, the annual revalidation of the site, and eventual decommissioning of the site.

The service will additionally provide the health monitoring for all Websites covered by this service to fast response

Value Proposition: Internet Website Publishing and Protection Service adds value to NATO through the central oversight of the process to publish NATO.INT and NATO affiliated websites to the Internet. This oversight adds value through the application of NATO Web Application Security Directive, secure public certificate issuance and continual site attribution.

Service Features:

- NATO Security Directive Coordination
- Web Application Security Remediation Coordination
- NATO.INT Internet DNS Publication
- Public PKI Certificate Issuance
- Content Delivery Network (CDN)
- Denial of Service Protection
- Continuous Site Oversight
- Website Decommissioning

Service Flavours: The service is in support of the Web Governance Directive and applies to each site requested to be publicly accessible over the Internet with NATO.INT domain name. Additional NATO affiliated sites may also subscribe to this service.

- **INF053-1 Standard:** The standard service flavour is for average website with expected average activity. This will provide the coordination activities required to publish the site on the Internet, two public PKI certificates (CDN edge and the origin server), cloud based content delivery network coverage, denial of service protection, revalidation of website with site owners and eventual decommissioning of the website.
- **INF053-2 Flagship:** The flagship service flavour is for NATO Flagship websites with expected heavy activity. This will provide the coordination activities required to publish the site on the Internet, two public PKI certificates (CDN edge and the origin server), cloud based content delivery network coverage, denial of service protection,



revalidation of website with site owners and eventual decommissioning of the website.

Available on:

Internet

Service Prerequisites:

None

Standard Service Support Level: N/A

Service Cost / Price: The unit of measure is per site (URL).

INF055 DCIS - Mission Adaptable Reference System (MARS) Service

Service ID: INF055

Service Name: DCIS – Mission Agnostic Reference System Service (MARS)

Portfolio Group: Infrastructure Services

Service Description: The Service enables the off-line, development, testing and acceptance of new hardware, software and mission baselines on multiple CIS domains in primary support of the Change Management and Release and Deployment Management processes.

MARS Service will enable a full range of newly fielded products and applications to be tested without interference and risk to the mission production environment.

Value Proposition:

INF055 Service will enable full customer testing and acceptance confidence when new capabilities are introduced into the DCIS environment. MARS will replicate the operational DCIS Anchor Nodes Service where the full range of user COI and COI services can be tested for compliance and compatibility with existing baselines.

MARS Service will be the hub that existing /future NDD reference systems will connect into for end to end testing and validation.

MARS Service will enable full referencing activities without any risk to the operational domain.

This service, aligned with the NATO Digital Backbone concept, is the very core of DCIS Multi Domain Operations, supporting warfighters from the strategic centre to the tactical edge.

The customer will have direct access to the Agency Service Management team for Deployable CIS and will be supported as described in the OTH004 Service Description.

Service Features:

Included NCI Agency Services: listed for each specific flavour in the Service Flavour section.

Included NCI Agency Services correspond with standard NCI Agency services, as described in respective service definitions. However, due to the deployable nature of the entire Deployable Nodes Anchor Service, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences are to be elaborated in detail within the respective service provisioning agreement. Delivery cost of these services differs from the standard service rates, and it is entirely included within the Deployable Nodes Anchor Service delivery cost.

Included CIS Assets: If applicable, listed for each specific flavour in the Service Flavour section.

Included Non-CIS Assets: If applicable, listed for each specific flavour in the Service Flavour section.

Reporting: This service is not actively monitored but monitoring can be requested.

Configuration Changes:

Major – Defined as a significant change to the service, such as complete re-configuration of all or majority of key configuration items (change of the service baseline), primarily in order to prepare a service for a new mission.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability.

MARS Service, by definition, will undergo multiple configuration changes as routine business. Nevertheless, MARS Service will follow the same Change Management process as the live environment

Maintenance:

Preventative Maintenance Inspections (PMI) – Where applicable, PMI to the Service are conducted in coordination with Customer to take into account any impact on scheduled testing and validation.

Corrective Maintenance Inspections (CMI) – CMI is undertaken by Provider in the event of Service asset failure, in accordance with the Customers' requirements as described in the service provisioning agreement.

Additional options: Increase in Service Availability; Change to Service Restoration Period.

Service Flavours:

MARS (INF055) – as described above.

Maintenance is conducted at support Levels 1-3 (L1-L3), and it includes regular sustainment of used applications and related licenses.

Available sub-flavours:

- None

Included CIS Elements:

- Network connectivity to other DCIS Reference Systems (DF, FF)

Included CIS Assets:

- Transmission and Network layer routing with redundancy;
- Distribution Layer Switches;
- Border Protection Firewalls;

- Voice Call Managers;
- VTC Collaboration Systems;
- Crypto Equipment.

Spare parts: This Service includes required stock of support L1-L3 spare parts, as specified in the service provisioning agreement.

Obsolescence Management: Obsolescence Management consideration for this service have been included in the service rate.

Available on: This Service will provide reference environment for:

NATO Unclassified Domain
NATO Secret Domain
Multiple Mission Secret Domains

Service Prerequisites: None, unless specified in the Service Flavours section for specific flavours.

Service Support Levels:

Service Availability Target: In accordance with the stipulations of the service provisioning agreement and based on the Customer requirements, INF055 is costed at, and measured against, standard support levels.

Service Restoration Period: In accordance with the stipulations of the service provisioning agreement, INF055 service restoration will be determined by the contracted level of service support.

Service Cost / Price: The unit of measure for the Service is Per System. Price details available in the Service Rates document.

INF056 DCIS Nodes – Deployable CIS Nodes for Maritime Based Users (MBU)

Service ID: INF056

Service Name: Deployable CIS Nodes for Maritime Based Users (MBU)

Portfolio Group: Infrastructure Services

Service Description: This Service provides Standardised and Certified Deployable Communication and Information Systems (DCIS) Nodes for the Maritime community. The Service provides the infrastructure and platform for a deployable CIS capability with inherent characteristics of modularity, scalability, sustainability, and interoperability. Each customer can adapt the Service to meet specific operational requirements through selection of the required workplace and application services. The customer can select those services from the workplace and application services sections of the Customer Costed Service Catalogue.

This service has includes enhanced cyber defence capability.

Value Proposition:

In peacetime location the service enable NATO to demonstrate a high readiness posture.

When deployed to the Maritime environment, the services enable NATO Warfighters to make the timely decisions for Mission Success.

The customer will have direct access to the Agency Service Management team for Deployable CIS and will be supported as described in the OTH004 Service Description.

Service Features:

Included NCI Agency Services: listed for each specific flavour in the Service Flavours section. Included NCI Agency Services correspond with standard NCI Agency services, as described in respective service definitions. However, due to deployable nature of the entire DCIS Nodes Service for Maritime Based Users, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences will be described in detail within the respective service provisioning agreement (i.e. SLA, SSP, TA, etc.). Delivery cost of these services differs from the standard service rates, and it is entirely included within the DCIS Nodes Service cost.

The DCIS Nodes Service for Maritime Based Users can host a variable number of Users (workplace services) and Application Services (Functional Area Services, FAS). The customer can select the specific requirements for the workplace and application services using the service catalogue, at additional cost.

Included in the service rates are the workplace services and applications for the system administrators to perform their duties.

Included CIS Assets: listed for each specific flavour in the Service Flavours section.

Included Non-CIS Assets: listed for each specific flavour in the Service Flavours section.

Reporting: Manually generated, no automated 24/7 monitoring of the Service status/availability is feasible.

Configuration Changes:

Major – Defined as a significant change to the service, such as complete reconfiguration of all or majority of key configuration items (change of the service baseline), primarily in order to prepare a service for a new mission. The standard change of the service baseline, costed as one complete change every two years. The schedule of Major Changes are agreed by both Provider and Customer in advance. The configuration baseline is made available to the customer through the Configuration Management Database.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability. Configuration and maintenance of the backup capability included.

Maintenance:

Preventative Maintenance Inspections (PMI) – The PMI to the Service are conducted at support Level 3 (L3) and in coordination with Customer to take into account the impact on operational availability and requirements, as a standard, along with configuration changes schedules taking into account manufacturer's instructions on maintenance, or otherwise defined technical maintenance standards;

Corrective Maintenance Inspections (CMI) – CMI is undertaken by Provider in the event of Service asset failure, at support Level 3 (L3) and in accordance with the Customers' requirements as described in the service provisioning agreement. This includes replacement of non-reparable equipment, where applicable under NATO financial rules and regulations.

Maintenance includes regular sustainment of used applications and related licenses.

Obsolescence: Service rates include the obsolescence management that standardizes the service rate. The obsolescence requirement will be amortize obsolescence funding over a rolling 5 year period.

Shipment and transportation: Service assets will be provided at Customer's disposition at any of customer's permanent locations. Full shipping between the repair and peacetime location is included.

Documentation: Customer will be provided with required technical documentation, as specified in the service provisioning agreement.

Spare parts: Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the required/mission state. Provider holds sufficient spares needed for Agency scheduled maintenance and anticipated incident resolution at the level to meet

the service needs. Local users hold L1 spare parts in accordance with recommended spare part list provided in the specifications for each system.

Security Accreditation Documentation: Customer will receive prepared documentation required for the Security Accreditation.

Service Flavours: The flavours of the Service are designed with different capabilities to effectively meet all operational scenarios. Each flavour includes additional options to enable full adaptation of the Service to the operational requirements. Options are to be requested by the customer through the annual submission of the requirements changes, in accordance within the established and/or agreed requirements establishment and budgeting process. Any in-year change of options shall be dealt with in accordance with the procedures agreed within the service provisioning agreement. Costing of options is conducted on per request basis.

The flavours of the Service represent specific tailored requirements for customer needs. Services included in the Deployable CIS Nodes for Maritime Based Users Service (DCIS Nodes for MBU Service) are:

INF057 Service - Maritime Command and Control Platform (MARC2P) Service

Former name of the service: SNFC2P/MARC2P (PLT012)

Maritime Command and Control Platform (MARC2P) is a medium deployable point of presence service providing deployed CIS and C2 services designed to be installed on maritime vessels. The INF0xx service includes provision of remote support to the MARC2P service throughout its deployment and on board maintenance and support in exceptional circumstances. MARC2P Service requires one instance of INF027 Mission Preparation Centre (MPC) per static maintenance facility of the service. The MPC service capability is essential to support the operational requirement for 48 hours or 5-days notice to move. In support of the DCIS mission preparation, the Provider conducts overall management of all services, to include enabling the distribution of Mission-specific configuration updates, system patches, security patches and updates. Deployment of MARC2P onto a vessel, including coordination of connectivity, can be requested separately through ordering SME008 Maritime Operational CIS Deployment and Recovery Service. MARC2P service requires connectivity through the existing CIS architecture of the hosting vessel, which is outside of scope of INF057.

Flavours:

INF057-1 MARC2P-1 Single Domain (SD) (Legacy SNF Kit) Service provides a single domain deployable NATO instantiation of the Bi-Strategic Command Automated Information System (Bi-SC AIS) Communication and Information Systems (CIS), enabling delivery of bespoke maritime Command and Control (C2) services (as specified in the service agreement) for up to 20 users.

INF057-2 MARC2P-2 Dual Domain (DD) provides maritime C2 services (as specified in the service agreement) in two (2) security domains: up to 22 users in the classified domain; and up to 5 users in the unclassified domain. MARC2P-2 (DD) service connects through the operational anchor functions and the deployable gateway.

INF044 Secure Maritime CIS (SEMARCIS)

SEMARCIS Service - a small deployable or static point of presence providing user secure access communication and information systems (CIS) as well as the corresponding services enabling command HQ and deployed commands to exercise Command and Control (C2) between NATO and non-NATO Nation (NNN) vessels in a NATO Operation/Mission/Exercise. Deployment of SEMARCIS to a vessel or static location, including coordination of connectivity, can be requested separately through ordering SME008 Maritime Operational CIS Deployment and Recovery Service.

Flavours:

INF044-1 SEMARCIS

SEMARCOM provides a single user, single domain system integrated into transport cases capable of supporting low intensity operations. It supports the parallel use of Inmarsat FleetBroadband Streaming, IP background and PSTN calls (all 3 services concurrently). The Service is provided with Broadband Global Area Network (BGAN) satellite terminal. It provisions the user equipment for 1 user that cannot be augmented.

SEMARCIS is a small deployable point of presence provides increased functionality. SEMARCIS provides interoperability with SEMARCOM plus enhancements providing up to 2 users to include: An additional Ethernet switch and an additional backup Firewall at the NDOG to improve system continuity. SEMARCIS is capable of exchanging secure, mission critical information between the NATO Command platform and the maritime assets provided by Non- NATO Nations. A fall-back over BGAN to MARCOM will be configured to appropriate server in Jchat, web browser, or VoIP phone. The Service does not include any non-CIS assets. It provisions the user equipment for 2 users that cannot be augmented.

INF044-2 Non-NATO Maritime Operation Centre (NNMOC)

NNMOC is a static option of the SEMARCIS service (expected in 2026) capable of exchanging secure, mission critical information between the NATO Command platform and the maritime assets provided by Non-NATO Nations via a static connection to MARCOM. Service includes Jchat, web browser, and VoIP phone. The Service does not include any non-CIS assets. It provisions the user equipment for 6 users that cannot be augmented.

INF059 Maritime CIS Platform (MARCISP) MARCISP service is a multi domain medium point of presence integrated into transit cases or built into 19" racks, meets the requirement for a Joint Task Force (JTF) deployed on-board a NATO vessel in support of a Maritime heavy operation. The system can operate self-sustained without reach-back to the data centre, provides standard user services and capable of hosting a limited set of FAS applications, supports up to 110 users. Interconnects using SATCOM provided by the hosting vessel. Dependent on the hosting vessel to provide sufficient electric power and cooling. Provisioned with the user equipment for the user requirements specified within the respective service provisioning agreement (i.e. SLA, SSP, TA, etc.). The flavours of the service represent specific tailored requirements for customer needs. Deployment/disconnection and demounting of MARCISP to a vessel, including

coordination of connectivity, can be requested separately and comes with change of cost of the provided services and may be handled separately through Customer Request Form process.

DCIS Nodes for Maritime Based Users Feature Table

Feature/Option	MARC2P-1 SD NS (Legacy SNF)	MARC2P-2 DD	SEMARCS	NNMOCs	MARCISP
General					
Maintenance and repair of non-CIS equipment and supply of L1 – L3 system spare parts and consumables, including also crypto spares, is included within the funding specified in the service provisioning agreement.	X	X	X	X	X
Maintenance/ sustainment/ replacement of UPSs	X	X	-	X	X
Included NCI Agency Services					
WPS001 Managed Devices Service - Laptop	X	X	X		X
WPS009 Voice Collaboration Service					X
WPS010 Video (VTC) Collaboration Service					X
WPS012 E-Mail Service					X
INF003 Enterprise Internet Access Service					X
INF007 Infrastructure Storage Service					X
WPS007 Print/ Scan/ Copy Service					X
INF016 Infrastructure Backup/Archive Service					X
INF001 LAN Service					X
INF002 NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service (only WAN Infrastructure Assets feature)					-
INF005 Infrastructure Integration Service					X
PLT001 Information Sharing and Collaboration Platform Services					X
PLT003 Web Hosting Service					X
PLT006 Database Platform Service					X
WPS014 Secure Voice Service					X
APP029 Military Message Handling Application Service					X
Included CIS Assets					
Virtual COM	X	X	-	-	X
IEG-B and IEG-C	-	?	-	-	X
Break Our Boxes (BOB)	-	-	-	-	X
MS Core	-	-	-	-	X
NU/MU Core	-	X	-	-	X
NS/MS Core	X		X	X	X
SATCOM Modems	-	-	-	-	-
Deployable SATCOM System (Sailor 250)			X	X	-
Crypto Assets	-	-	-	-	X
Helpdesk Assets	-	-	-	-	-
NAS	X	X	-	-	X
µISM	?	?	-	-	X

Feature/Option	MARC2P-1 SD NS (Legacy SNF)	MARC2P-2 DD	SEMARCIS	NNMOCs	MARCISP
Intra Nodal Distribution System (INDS)	-	-	-	-	-
Service Access Points (SAP)	-	-	-	-	-
Cyber Defense	X	X	-	-	X
Element Network Manager (ENM)	-	X	-	-	-
Integrated Network Management System (INMS)	-	-	-	-	-
Interface to Nations Module (INM)	-	-	-	-	-
Included Non-CIS Assets					
Power Generator	-	-	-	-	-
Environmental Control Unit (Provided and Supported by host location*)	*	*	*	*	*
Racks (Provided and Supported by host location*)	*	*	*	*	*
Uninterrupted Power Supply (UPS)	X	X	-	-	X
Transit case	X	X	X	X	X
Tent (with Furniture)	-	-	-	-	-
Manual Handling Equipment	-	-	-	-	-
Available Options (comes with change of cost of the provided services and may be handled separately through Customer Request Form process)					
Additional Baseline Changes	X	X	-	-	X
Increase in Service Availability	-	-	-	-	-
Change to Service Restoration Period	-	-	-	-	-
Additional Domain Change		X	X	X	X
Functional Area Services (FASs to be specified within the service provisioning agreement)	X	X	-	-	X
ISO standard transportation containers	-	-	-	-	-
Domain Availability					
Single domain	X	-	X	X	X
2 Simultaneous Domains	-	X	-	-	X
3 Simultaneous Domains	-	-	-	-	X

INF060 GP DCIS – General Purpose Deployable CIS

Service ID: INF060

Service Name: General Purpose Deployable CIS

Portfolio Group: Infrastructure Services

Service Description: This Service provides Non-CIS Assets: General Purpose (GP) Tents, Environmental Control Unit (ECU), UPS, Power Generators, Racks, Power Strips in order to support use of DCIS Nodes in both peacetime locations and deployed.

Value Proposition:

The service provides Non-CIS assets such as tents, BC protection and ECU, UPS, Generators and manual handling equipment to enable operation in harsh environments between -30° and +49° Celsius.

Service Features:

This Service provides Non-CIS support to the following Service Flavours:

Feature/Option	DragonFly	CGS	LINC-E	IMCD	ACP	RNM	Mini-PoP	TLK/ILK
General								
Maintenance and repair of non-CIS equipment and supply of L1 – L3 system spare parts and consumables, including also crypto spares, is included within the funding specified in the service provisioning agreement.	X	X	X	X	X	X	X	X
Maintenance/ sustainment/ replacement of UPSs	X	X	X	X	X	X	X	
Included Non-CIS Assets								
Power Generator		X		X				
Environmental Control Unit	X	X	X	X				
Power Generator Set (PGS)			X*					
Cargo Transport Cases	X*	X*	X*	X*	X*	X*	X*	X*
Racks					X*			
Uninterrupted Power Supply (UPS)	X	X	X*	X*	X*	X	X	X
Transit case	X	X	X	X	X	X	X	
Tent (with Furniture)	X	X	X	X				
Biological Chemical Tent and Filters	X							
Manual Handling Equipment	X							
Operators and maintainers completed the Agency approved training.	X	X	X	X	X	X	X	X
Customer ensures the provision of secure facility to enable operation	X	X	X	X		X	X	X

* Number of assets depending on the chosen options

** Number of assets depending on the requested operational configuration

Documentation: Customer will be provided with required technical documentation, as specified in the service provisioning agreement.

Spare parts: Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the factory state. Provider holds sufficient spares needed for Agency scheduled maintenance and anticipated incident resolution at the level to meet the service KPIs. Local users hold L1 spare parts in accordance with recommended spare part list provided in the specifications for each system. Local users are responsible to request replenishments through Provider's Material Request Procedure.

Service Cost / Price: The unit of measure for each of the Service Flavours that is supported by this Non-CIS Service is Per System.

INF062 NS MOBILE IT CAPABILITY – NSMOB – HERMES PACKAGE (HERMES)

Service ID: INF062

Service Name: NS Mobility NSMOB (HERMES)

Service Type: Customer Facing

Portfolio Group: Infrastructure Service Mobile and Multi-Domain Access

Service Status: Pipeline

Service Description: The HERMES Package provides to its users mobile access to the NATO Bi-Strategic Command (Bi-SC) Automated Information System (AIS) [Bi-SC AIS NS] network. It consists of two key components:

1. **HERMES Kit:** The HERMES Kits provide NATO personnel with a highly secure and mobile IT solution, multi-domain capable, ensuring protected access to NATO networks from any location according to the NOS approved Security Operating Procedures (SecOps). These accredited mobile Multi-Domain Workstations (MDW) leverage advanced SD-WAN technology to optimize connectivity across various network infrastructures, including commercial LTE/5G, Public Wi-Fi, and NATO's secure communications network.
2. **HERMES Anchor Function:** The HERMES Anchor Function serves as the secure and resilient backend infrastructure that enables NATO personnel to access classified networks and legacy NS services (see list in Service Prerequisites section below) reliably, regardless of their location. As a geo-redundant solution, it is strategically deployed across two secure NATO locations – Lago Patria (Italy) and Brunssum (Netherlands) – ensuring continuous availability, failover capabilities, and operational resilience even in the event of network disruptions or security threats.

Value Proposition: Seamless mobile access to existing NS tools previously only available on Static Bi-SC AIS network.

- **Secure Mobile Access:** The HERMES Package provides NATO decision-makers with secure, mobile access to NS network, access to applications, tools and information via an established CloudApp Gateway therefore minimum training overhead for Users already familiar with the Static services.
- **End-to-End Support:** fully integrated End-to-End support model, ensuring that all aspects of secure communication, connectivity, and operational readiness are properly supported.
- **High Availability & Scalability:** Designed to operate within NATO's C2 structure, ensuring 99.5% availability and future scalability.
- **Seamless Integration:** By embedding HERMES into the existing NCIA Enterprise Service Operations Center (ESOC), NATO personnel benefit from

a centralized, streamlined support structure that enhances service reliability, security, and responsiveness.

Service Features: The HERMES Package services are structured into key operational areas:

1. Enterprise Service Management and Control (SMC): Comprehensive service governance, Service Lifecycle Management and Service monitoring, including:
 - Service Asset and Configuration Management (SACM): Maintains an accurate inventory of all HERMES components and their operational configuration.
 - Field Support Service (FSS): On-site technical support and troubleshooting.
 - Monitoring Subservice (MON): Real-time system health and performance monitoring with alerting of issues to support personnel.
 - Centralised Service Desk (CSD) Subservice: Enabling single point of contact access to multi-tiered IT support.
2. Client Provisioning Services (CPS):
 - HERMES kit issue, initial setup and End User Training provided direct to End Users at Service Customer's location.
 - Available LTE/5G, Wi-Fi, LAN : Provides connectivity to end-user devices with SD-WAN access technology.
 - Endpoint Protection (EPP): Ensures security with real-time monitoring and threat detection.
 - Endpoint Provisioning (EPS): Automated deployment of devices with pre-configured security policies.
3. Cyber Security Service (CSS): Integrated Cyber Security services provided through NATO's Cyber Security Operations Centre (CSOC):
 - Log Aggregation (LogA): Centralized collection, monitoring and analysis of security-relevant data.
 - Online Computer Forensic (OCF): Digital forensic analysis of security incidents.
 - Online Vulnerability Assessment (OVA): Continuous unobtrusive security vulnerability and risk assessment scans.
4. Infrastructure as a Service (IS):
 - Backup and Recovery Service (BRS): Ensures data integrity and disaster recovery capabilities.
 - Hyper-Converged Infrastructure (HCI): Optimized computing and storage platform.
 - Infrastructure Network Subservice (INS): Manages NS Mobility access to NATO-compliant network services.
 - Remote Access Subservice (RAS): Secure remote access to NATO systems.
5. Enterprise Core Services (ECS):
 - Database Service (DBS): Scalable and secure SQL database management.
 - Directory Service (DIR): Centralized identity and access management (iDAM) via maintained Active Directory services.
 - Unified Communication Subservice (UCC): Secure video, voice, and messaging platform and integration to Enterprise communication services.
 - Email Messaging Service (EMS): Enterprise-grade Microsoft Exchange email services for Admin / Support communications.

6. 24/7 Health and Performance Monitoring
 - Available for all critical systems that require continuous operation
 - Monitored by the SMC Monitoring Subservice with automated alerting upon failure and triggering based on predefined thresholds
 - Critical Incident submission via the NCIA ESOC CSD.
 - Emergency 2nd Level response teams on on-call standby support outside of Regular Business Hours
7. Support Service Contact: Single Point of Contact: NCIA ESOC CSD Support
8. On-Demand Field Service Support:
 - Dedicated field engineers are deployed to Peace Time Locations (PTL) NATO locations to provide support to Hermes-KIT End-user, system diagnostics, maintenance, incident resolution and Training.
9. On-Demand Field Service Support:
 - For Extended On-Site & Custom Support outside PTL – best effort

Service Ordering and Request:

- Service Requests: Requests for HERMES kits should be submitted via ESOC CSD using self-service access to the NCIA Enterprise BMC NS ITSM toolset and support structures.
- Service Desk: 24/7/365 Level 1 support service accessible via existing NCIA ESOC CSD contactable by phone, email, and web portals.

Service Flavours: This Service is available as a Single Flavour

Available on: NS – Mobile Kit

Service Prerequisites:

- WPS002 – Enterprise Identity and Access Management (iDAM).
 - Valid NS AIS account is required, ensuring that only authorized NATO personnel can access and utilize the service
- WPS008 - Integration with NCIA Enterprise Service Management & Control (SMC) and NATO's Enterprise Service Operations Centre (ESOC).
- INF003 – Enterprise Internet Access Service.
- Access to NATO WAN / SDN environments & managed Infrastructure services.
- Cyber Security (SEC) Monitoring & Incident Mng services operated by NCSC.
- Compliance with NATO Security Accreditation via SEC001)
- PLT011 – Cloud Access Application (CloudApp) Service.
- Note: The following legacy NS services are accessed by HERMES Users:
 - NS Portal Services: NIP [APP086]; EDMS [APP031]; TT+ [APP030].
 - WPS010 - Video VTC Collaboration Service
 - WPS014 - Secure Voice Service
 - APP015 – JCHAT Application Service
 - APP022 – NCOP Application Service

Standard Service Support Levels:

- Level 1 (L1): Initial user support and troubleshooting via ESOC CSD.
- Level 2 (L2): Technical assistance from service specialists.

- Level 3 (L3): Support from OEMs and advanced engineering teams.
- Level 4 (L4): Manufacturer / vendor-level fixes and system enhancement.

Service Availability¹ Target: CSLA agreed KPIs for CloudApp consumed services

1. HERMES Anchor Function: 99.5% inherent availability (Ai) / 99.0% operational availability (Ao) based on 24/7/365 operation.
2. HERMES Kit: As designed availability limited by COTS reliability (i.e. vendor's Mean Time Between Failures).

Service Restoration:

1. Priority 0 (P0) / Priority 1 (P1) Incidents: Resolution within 4 hours (24/7).
2. Priority 2 (P2) Incidents: Resolution by the Next Business Day (NBD).
3. Priority 3 (P3) Incidents: Resolution within 5 working days.

Service Reporting: *describes standardised service reporting to customers in accordance with the NCI Agency SLAs*

Available NCI Academy Training not covered by service cost: NO

Service Cost / Price:

- Pricing Model: Monthly service fee based on system coverage and SLAs.
- Customization: Additional costs apply for Extended On-Site & Custom Support outside PTL – best effort.
- Service Rates List: Will be available in the NCIA Costed Customer Service Catalogue.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes



Platform Services



This page is left blank intentionally

PLT001 Information Sharing and Collaboration Platform Services

Service ID: PLT001

Service Name: Information Sharing and Collaboration Platform Services

Portfolio Group: Platform Services

Service Description: This service offers NATO entities platforms to create, collaborate on, and share information both internally within the Alliance and externally with partners. It provides secure online portals and websites where users can create, store, manage, distribute, publish, view, and search all kinds of digital content. Customers can build a rich and robust collaborative environment by leveraging web information publishing and portal features. The service enables collaboration and social interaction within various groups, including teams, communities, the NATO Enterprise as a whole, individual NATO and PFP nations, Industry, and Academia.

Value Proposition: This service empowers NATO entities and their partners to collaborate seamlessly and securely, fostering efficient information and knowledge sharing. By providing platforms/portals with robust tools for content creation, management, and distribution, it streamlines workflows, enhances communication, and breaks down information silos. This, in turn, facilitates better decision-making, accelerates project delivery, and ultimately contributes to the NATO's mission by maximizing the impact of its work through effective information knowledge management (IKM) in compliance with NATO IKM and security policies.

Service Features: Subject to the specific service flavours, this service provides the following features

1. Content Management:
 - Sites is where all collaboration happens. Sites contain many features, including the capability to create, store, and retrieve data, and manage, tag and search for content and information.
2. Document Management:
 - Allows document collaboration with rich document experience on co-authoring, version control and secure sharing.
 - Connectivity with Microsoft Office client applications through lists and document libraries.
 - Apps for SharePoint, workflows, Word or Excel Services.
3. Social:
 - Provides social networking capabilities, newsfeeds, and profile searching and tagging, along with the capability to search, locate and interact with people through their skills, organizational location, relationships.
 - Blogs, wikis, surveys, metadata tags and other.
4. Search: the ability to search content from multiple sources, fine-tuned with facets, filters and autocomplete.
5. Staging environment to assist with capturing customer functional requirements or executing User Acceptance Tests (available on request).

Service Flavours: The Service is available in seven flavours:

The NATO Enterprise Collaboration Platform: A platform built using "NATO Enterprise Portal Templates" which act as building blocks, allowing users to easily design and manage their sites. These building blocks include options like landing pages, exercise areas, document collaboration spaces, project sites, event pages, and more. The templates incorporate the NATO visual identity, pre-configured NATO web parts, and standard document metadata compliant with the "NATO Core Metadata Specification" (NCMS), simplifying use and improving accessibility. The platform scales to SharePoint's full storage capacity, requires no downtime for updates, and is responsive across mobile phones and tablets. The default storage is 10 GB¹.

Best for: Customers who require sites with publishing or/and collaboration features with a high degree of autonomy for designing and content authoring while aligning with the NATO metadata and look and feel standards.

Four flavours are available for platforms on unclassified and classified networks, as well as small and large options (see Service Cost / Price section for more details):

PLT001-A1 NATO Unclassified Enterprise Collaboration Platform Small

PLT001-A2 NATO Unclassified Enterprise Collaboration Platform Large

PLT001-A3 NATO Classified Enterprise Collaboration Platform Small

PLT001-A4 NATO Classified Enterprise Collaboration Platform Large

Bespoke Publish/Collaboration Portal: A fully custom-made site with a dedicated URL address and selected advanced features specifically tailored to customer requirements in terms of functionality, technology and processes.

Best for: Customers who require specific functionalities not available in the "out of the box" offering advanced features, such as custom metadata, custom look and feel and content management features, sophisticated workflows, fine-tuned security (by user, documents or shared spaces) or integration with other applications. This offered in a single flavour:

PLT001-B Bespoke Publish/Collaboration Portal²

Communities of Interests (COI) Collaboration Platform: Community of Interest (COI) sites share a common URL structure within the COI portal. They aim to enhance collaboration within and between NATO Communities of Interest (e.g., Electronic Warfare, Space, Cyber Security, CIS, Exercises, and more). Designers created the information architecture and tools to strengthen teamwork within these subject-focused collaboration spaces and enable information exchange between different communities. Both NATO and non-NATO entities, including nations, industry, and academia, can access COI sites, supporting cooperation

¹ Can be increased, based on customer requirements and subject to an additional cost of the underlying prerequisite services for the additional storage.

² There is no separate rate for Classified and Unclassified Portals because the operation and maintenance costs are determined per instance during the price proposal creation.

between the NATO and its external partners. These COI sites follow the predefined NATO Visual Identity and comply with the "NATO Core Metadata Specification" (NCMS). The default storage size is 4 GB .

Best for: Customers who require quick delivery of a collaboration environment focused on common professional interest (Communities of Interests) or/and those who wish to work together with NATO External Partners.

Two flavours are available for platforms on unclassified and classified networks

PLT001-C1 NATO Unclassified Communities of Interests (COI) Collaboration Platform

PLT001-C2 NATO Classified Communities of Interests (COI) Collaboration Platform

Available on:

	PUBLIC	UNCLASSIFIED	RESTRICTED	SECRET	MISSION SECRET
NATO Enterprise Collaboration Platform	X	X	X	X	X
Bespoke Publish/Collaboration Portal	X	X	X	X	X
Communities of Interests (COI) Collaboration Platform	X	X		X	

Service prerequisites:

Service prerequisites depend on the underlying infrastructure and on the specific service flavour.

- NDW001 NATO Digital Workplace Service (Low Side) or NDW002 NATO Digital Workplace Service (High Side)
- WPS003 Enterprise User License Service
- For Classified-Content services hosted on NATO Infrastructure
 - o PLT003 Web Hosting Service
 - o PLT006 Database Platform Services
- For Unclassified-content services hosted on NPCL NATO Public Cloud
 - o PLT010 Cloud Services Management and Integration Services

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration Priority: P3.

The Standard Service support comprises the following activities:

- **Operation:** application monitoring, log management, batch jobs management, backup & restore, auditing, Service Requests fulfilment.
- **Corrective Maintenance:** diagnosis and removal of the causes and the effects of any malfunction affecting the Service.
- **Preventive Maintenance:** preventive actions needed to avoid future malfunctions
- **Adaptive Maintenance:** adjustment of the Service in order to adapt to the minor changes of the sub system components (i.e. Operating System, Database Management System, Browser, SharePoint and SharePoint add-ons). Major changes of the sub system components can be requested via dedicated projects.

Service Cost / Price:

The unit of measure for the Service is “per URL”, and more specifically:

- For the **NATO Enterprise Collaboration Platform** the unit of measure is per each SharePoint “Site Collection”. The price depends on the type of “Service Plan” chosen by the customer, as per the following table:

Service Plan	Number of registered users	Number of Service Requests/Year
Small	Maximum 100	Up to 6
Large	Unlimited	Up to 12

The table above shows that every Service Plan enables the customers to have a maximum number of registered users and to ask for a maximum number of Service Requests per year.

- In the case of the **Bespoke Publish/Collaboration Portal**, the unit of measure is per site. Since it is a tailored solution, the customer requests it via CRF, after which both the service initiation costs and O&M costs are established in a price proposal.
- In the case of the **Communities of Interests (COI) Collaboration Platform**, the unit of measure is per each Community of Interest “Site”.

The cost of the Services does not include the cost of all the underlying service prerequisites. The total amount of the service delivery price is charged in accordance with specifically arranged conditions of the service delivery

PLT002 Combined Federated Battle Laboratory Network (CFBLNet) Service for NATO Organisations

Service ID: PLT002

Service Name: Combined Federated Battle Laboratory Network (CFBLNet) Service for NATO organisations

Portfolio Group: Platform Service

Service Description: The Combined Federated Battle Laboratories Network is a multinational, research, development, training, trials and assessment infrastructure for C4ISR, based on a multinational IP backbone with managed enclaves on top in support of the initiatives. Infrastructure reuse for multiple multinational and concurrent initiatives is a key element for the CFBLNet mission partners. CFBLNet operates as a true federation; no single nation owns the CFBLNet, where each member is responsible for provisioning and operation of its own sites and systems. CFBLNet fulfils the need for persistent joint multinational and cost effective infrastructure. The capability allows for various partnerships; CCEB, NATO, bilateral and multilateral. CFBLNet was established in 2001 and is continuously improving its services to provide the best and most cost effective federated infrastructure in support of its mission. Currently its scope consists of 38 mission partners: all 30 NATO Nations and Austria, Australia, Finland, New Zealand, Sweden, Switzerland, European Union External Action Service EEAS (EUMS) and the NATO organization. CFBLNet is open through sponsorship to additional partner nations. As a prerequisite, customers are asked for valid security accreditation and related MSAB Site and Initiative National/NATO accreditation endorsement certificates (S-, I- NAEC's).

Value Proposition: CFBLNet provides the Multinational federated coalition network infrastructure of choice to facilitate all potential non-operational activities to support the war fighter. The single CFBLNet network infrastructure with many partners and initiatives, saves cost, increasing their quality, lower their risk and reduce setup time. CFBLNet offers an agile and fully service based non-operational network infrastructure, and operates at up to a Secret releasable accreditation level. CFBLNet provides common framework, well defined processes, security procedures and agreed technical standards.

Service Features: The Combined Federated Battle Laboratory Network (CFBLNet) Service offers the following features:

- Access points (connection to Core up to 50Mbps)
- Network Services (Routing, encryption, switching, DNS, NTP, network management, testing)
- Service Desk (3hrs/month)
- Coordination with Nations
- Coordination for NATO
- Initiative / CIIP support
- Limited email (<20 accounts)
- Chat in standing enclaves (Chat server)
- Web Services for initiatives (Microsoft Web server)

- VOIP (Cisco Voice server)
- VTC in standing enclaves (VTC MCU in RED, Pink and CUE enclaves (Acano/Cisco or other))
- SharePoint in standing enclaves (Sharepoint server)
- Data Diodes (Low-> High file transfer)
- Anti-virus / WSUS (Antivirus and Windows update servers for automatic updates (AFPL approved and regular versions)
- Simulation of CFBLNet (optional) (simulation of nation/organisational node for testing)
- Flow audit in standing enclaves
- Additional access bandwidth (optional)

Service Flavours:

1. PLT002-1: CFBLNet for NATO organizations only – BASE
2. PLT002-2: CFBLNet for NATO organizations only – Extra NKIT

- A. During initiatives
- B. Outside initiatives

Features	Flavour 1
NATO Organisations	
Core Access Points	
NATO Access points	•
Network Services	•
Service Desk	•
Coordination with Nations	•
Representation for sponsored nations	
Coordination for NATO	•
Initiative / CIIP support	•
Limited email	•
Chat in standing enclaves	•
Initiative Web Services	•
VOIP	•
VTC in standing enclaves	•
SharePoint in standing enclaves	•
Data Diodes	•
Anti-virus / WSUS	•

Simulation of CFBLNet (opt)	●
Flow audit in standing enclaves	●
Full local access node provisioning and operation	●
Additional access bandwidth	●

Available on:

CFBLNet NS
NS (REL)
NR (REL)
NU
NU (REL) for various NATO and Coalition communities

Service Prerequisites:

NATO Organisational subscribers: Link between NATO Organisational CFBLNet Access Node and NATO CFBLNet PoP infrastructure through NGCS/LTX. (Alternative if NCGS is not possible: leased line, satcom, alternative linkage).

The European and NATO CFBLNet NOC/PoP has link termination points at an Amsterdam (commercial DC), NATO HQ (NGCS/LTX), NCIA Mons (NGCS/LTX) and NCIA The Hague (NGCS/LTX and commercial).

Standard Service Support Levels:

Service Availability¹ Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Nations and non-NATO organisations which would like to subscribe to “national” CFBLNet services are handled through a CRF and subsequent FFP quotation. PLT002 is not applicable to Nations and non-NATO organisations.

¹ The minimum “Monthly Uptime Percentage” for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

PLT003 Web Hosting Platform Service

Service ID: PLT003

Service Name: Web Hosting Platform Service

Portfolio Group: Platform Services

Service Status: Available

Service Description: Web Hosting Platform Service enables fully managed and scalable hosting platforms (on-premises / off-premises) for web based solutions. The service also provides high availability, and a disaster recovery mode for customers seeking greater performance and reliability. General features of the service include: scalability, security, availability, interoperability and performance monitoring. The service is delivered as shared or dedicated flavours on one of the following supported web hosting platforms: Microsoft Internet Information Services (IIS), Apache, Oracle Web Logic and Microsoft SharePoint as a foundation in an internet/extranet environment.

Value proposition: Web Hosting Service offers multiple benefits:

- Scalability by ensuring availability of resources as the Web-based Application Service requires;
- Lower Total Cost of Ownership (TCO) of a Web-based Application Service provided through a shared and dedicated hosting model;
- Location Independence by accessibility of a Web-based Application Service from any location with Internet Connectivity, subject to security policies that would allow;
- Secure web hosting by default to prevent the any possible violations;
- No Single Point of Failure; if one service fails, the broader service can remain unaffected, ensuring service availability and reliability.

Service Features: The Web Hosting Service has the following features:

- Fully managed platform –dedicated or shared- , allows application owners to focus only on their application, and no need to worry about underlying environments;
- Operational support, including performance monitoring and expertise support but not limited to;
- Optional high availability and disaster recovery capabilities ensures availability and resiliency;
- Secure Web Application Services through Access Management (within the available standard options in Microsoft Internet Information Services (IIS), Apache, SharePoint, Web Logic);
- Support for standard web protocols, included but not limited to HTTPS (SSL);
- Three-tier architecture, separating presentation layer, application layer and database;
- Server side frameworks and supported middlewares, among others: Java, .NET, PHP, Ruby,
- NATO required security features and tools.
- Web/application servers: Apache and IIS;
- Provisioning of SharePoint as a foundation platform to support hosting of SharePoint based portals and applications on Intranet and Extranet.

Service Flavours: The Service is available in two flavours

- **Shared Web Hosting Platform :** A web hosting platform shared between different web sites to reduce the cost of underlying backend. Isolation and high availability is to be provided on platform level on premises and off premises (cloud). It is best for standard web sites that do not require high volumes of information, transaction, and when platform level privileges are not required.
 - **On Premises:** It is requested by amount of data size (minimum 10 GB). After the first 10 GB quota, it can be extended with 1 GB increments. High Availability is provided by default, but without disaster recovery. It is best for the web sites publishing sensitive data to NATO Enterprise.
 - **Off Premises (cloud):** It is requested by amount of data size (minimum 10 GB). After the first 10 GB quota, it can be extended with 1 GB increments with reduced rates. High Availability and Disaster Recovery are provided by default. The service rate includes underlying infra and security costs. It is best for the web sites publishing to public on internet.
- **Dedicated Web Hosting Platform:** A dedicated web hosting platform on isolated backend is to be provided to customer to make them able to design and manage the web sites on the platform with High Availability and/or Disaster Recovery option on premises. It is best for tailored web site that requires high volumes of information, transaction, or specific administrative privileges on the platform.
 - **Stand Alone:** It is requested by amount of data size (minimum 200 GB). There is no High Availability and Disaster Recovery provided. It is best for the non-business critical web sites those not requires high performance and availability
 - **With HA only:** It is requested by amount of data size (minimum 200 GB). There is High Availability implemented, but no Disaster Recovery. It is best for the web sites sensitive to performance and requires high availability.
 - **With DR only:** It is requested by amount of data size (minimum 500 GB). There is Disaster Recovery implemented, but no High Availability. It is best for the web sites that do not require high performance nor high level availability, but require quick recovery in case of loss of the service.
 - **With HA/DR** It is requested by amount of data size (minimum 500 GB). There is Disaster Recovery and High Availability implemented. It is best for the mission/business critical web sites that require high performance, high level availability, as well as quick recovery in case of loss of the service.

Available on:

- NATO Unclassified
- NATO Restricted
- NATO Secret
- Mission Secret
- Public Internet Access (PIA) Gateway (Security classification up to and including NATO Unclassified)
- Hybrid and Public Cloud (Security classification up to and including NATO Unclassified and NATO Restricted)

Service Prerequisites:

- PLT006 - Database Platform Services
- PLT010 - Cloud Services Management and Integration Service
- INF003 - Enterprise Internet Access Service
- INF004 - Infrastructure Hosting Service
- INF016 - Infrastructure Backup and Archive Service
- RLS001 - Real Life Support
- WPS002 - Enterprise Identity Access Management Service

Underlying Services: OTH001

Standard Service Support Levels:

	Availability Target	Service Period	Restoration
Shared Web Hosting			
On Premises	99.9%	8 hours (business)	
Off Premises	99.9%	4 hour (wall clock)	
Dedicated Web Hosting			
Without HA/DR	98.0%	27 hours (business)	
With HA only	99.9%	8 hours (wall clock)	
With DR only	99.0%	8 hours (business)	
With HA/DR	99.9%	4 hour (wall clock)	

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: Service cost is calculated based on the data size requirement. Service Unit (SU) is GB.

Please see Service Rates document for standard rates applicable to the service

PLT004 Service Oriented Architecture & Identity Management Service (SOA&IDM)

Service ID: PLT004

Service Name: Service Oriented Architecture & Identity Management Service

Service Type: Enabling

Portfolio Group: Platform Service

Service Status: Pipeline

Service Description: The Service Oriented Architecture & Identity Management is delivered as Platform-as-a-Service (PaaS) simplifies collaboration across the NATO Enterprise Business Applications. SOA&IDM platform makes the deployment, operation and maintenance more efficient and effective. The service follows the principles of service orientation, applying them to the design of the platform services themselves, and supports the transformation of silo-based CIS systems into an information systems that is fully aligned with the organisation, and is easily adapted to future demands.

Value Proposition: The SOA&IDM Platform will deliver reusable SOA&IDM middleware services. These services make application development simpler and more rapid, enabling easy and secure federation between NATO ecosystem applications, enhancing application innovation, maintenance and operation. As a result, it ensures that business applications across the Enterprise can efficiently and effectively respond to NATO's operational and static needs.

Service Features:

- **Agility:** The Platform will be available on the ON and PBN networks, and will allow Functional Services (FS) to be rapidly deployed and/or reconfigured in response to the requirements
- **Simplicity:** FS software developers in NATO will be able to focus solely on delivering capabilities that meet the needs of the users in the operational community, rather than also providing the middleware for those capabilities, including security and interoperability. This middleware is provided by the SOA&IDM Platform services.
- **Integration:** Service lifecycle will provide an integrated service delivery environment that facilitates automation, traceability and collaboration.

Service Ordering and Request: It is standard no exception.

Service Flavours: The Service is offered as a single flavour. (After service transition to the production, the unit based cost model will be analysed and used)

Available on:

- NATO Secret

Service Prerequisites:

- INF004 Infrastructure Hosting Service
- INF005 Infrastructure Integration Service

- INF006 NATO Enterprise Directory Service
- INF007 Infrastructure Storage Service
- PLT015 IV&V Reference Platform Service

Underlying Services: OTH001

Standard Service Support Levels:

Service Availability Target: 99.9% (during Support Hours) and 99.5 (outside of Support Hours)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 1 hour (during Support Hours) and 4 hours (outside of Support Hours).

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting: Service Reports will be based on the number of incidents (solved/failed), Service Request. Also availability figures will be populated from the service monitoring toolsets/features

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. Following the service transition to the production; service consumption and costs will be analysed to produce the Service Unit based cost model.

PLT006 Database Platform Service

Service ID: PLT006

Service Name: Database Platform Service

Portfolio Group: Platform Service

Service Description: Database Platform Service provides a fully managed database platform for use as an integral part of a production, testing, and/or development environment. The service provides flexible, scalable, and demand based platform, which is oriented toward central monitoring and management where underlying complexities of Database technologies (Oracle, MS SQL, MySQL, PostgreSQL and MongoDB) are encapsulated as a combined generic service.

Value Proposition: The Service offers the following benefits:

- Lowered Total Cost of Ownership of a database through the provision of a consolidated, standardized and volume managed database environment;
- Agility to meet NATO demands through provision of standardized, tested environments;
- Size and growth of a database monitored and provision of required capacity made to ensure continued availability and performance to meet operational needs;
- For standard use, the underlying technical complexities are isolated from the customers, technology agnostic;
- Increased security and availability through a dedicated team of experts who monitor the service

Service Features: Database Platform Service offers the user the following features:

- Database hardware capacity.
- Lifecycle management of the Database Platform.
- Database software licensing and maintenance.
- Centrally and fully managed, automated backup with point-in-time recovery.
- Software Lifecycle management for RDBMS, maintenance (including patching) and support.
- System, database and performance monitoring and tuning.
- Capacity provisioning through scalable and flexible management of available resources.

Service Flavours:

The Database Platform service offers two separate flavour categories for “Architecture” and “Technology” that complement each other. The respective sub-flavours of both categories must be selected simultaneously to define the requested architecture and the technology required to enable that architecture.

- **Architecture Flavours:** Architecture Flavours: Offers the structure of the required platform with the following sub-flavours. Technology Flavour must be chosen as a complementary to enable the selected architecture. The unit of measure for these flavours is “per GB”.

- **PLT006-1 Shared Database Platform:** Database platform shared between different database owners to reduce the underlying cost. Isolation and high availability are provided. Best for basic requirements that do not require high volumes of data, transaction, and situations when platform level-privileges are not required (such as system administrator). Minimum 10 GB is provisioned.
- **PLT006-2 Dedicated Database Platform:** An isolated and dedicated database hosting platform will be provided to the customer so that they can design and manage the data on the platform with High Availability and/or Disaster Recovery option. Best for tailored applications that require high volumes of data, transaction, or specific administrative privileges on the platform.
 - **PLT006-2A Standalone:** High Availability or Disaster Recovery are not provided. Best for the non-business critical applications that do not require high performance and availability. Minimum 350 GB is provisioned.
 - **PLT006-2B High Availability:** High Availability implemented, but no Disaster Recovery. Best for the performance sensitive and high availability required applications. Minimum 500 GB is provisioned.
 - **PLT006-2C Disaster Recovery:** Disaster Recovery implemented, but no High Availability. Best for the applications that do not require high level availability or high performance, but require fast recovery in the event of service loss. Disaster Recovery implementation is guaranteed not to be in the same data centre. Minimum 550 GB is provisioned.
 - **PLT006-2D High Availability and Disaster Recovery:** High Availability and Disaster Recovery implemented. Best for business critical applications that require high performance, high level availability, as well as fast recovery in the event of service loss. Minimum 700 GB is provisioned.
- **Technology Flavours:** Defines the technology required for the desired architecture with the following sub-flavours as a complementary to the selected Architecture flavour. The unit of measure for these flavour is “per Core”.
 - **PLT006-ENT - Enterprise Technology:** Best for Shared, HA and/or DR architectures, also good for high performance, high security, workload intensive Standalone architectures. MS SQL Server Enterprise Edition, MySQL Server Enterprise Edition and MongoDB Enterprise Edition are offered.
 - **PLT006-STD - Standard Technology:** Best for Standalone and HA architectures that require simple or very limited HA capabilities and non-intensive data processing. MS SQL Server Standard Edition is offered.

- **PLT006-GEN - General Technology:** Best for dedicated and simple test and development environments. Very limited in shared, HA and/or DR architectures. No vendor support or less than other technology types. MS SQL Server Developer Edition, MongoDB Community Edition, MySQL Community Edition and PostgreSQL Community Edition are offered.
- **PLT006-3 Oracle Licenses:** Based on Oracle's licensing policy, all physical processors connected to the network will be licensed. The unit of measure for this flavour is 1. Covered products are listed below. Formal request (through ITSM) required for use.

Oracle DB Ent. Ed.	Oracle Tuning Pack	Oracle Real Application Clusters
Oracle Active Data Guard	Oracle Analytics Server	Oracle WebLogic Server Ent. Ed.
Oracle Diagnostics Pack	Oracle Data Integrator Ent. Ed.	Oracle DB Lifecycle Mgmt. Pack

Available on:

NATO Unclassified (On-Prem and Off-Prem/Cloud)
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

WPS002 Enterprise IDAM Service
WPS003 Enterprise User License Service
WPS008 Enterprise Service Operations Centre
INF004 Infrastructure Virtualization Service
INF005 Infrastructure Network Service
INF007 Infrastructure Storage Service
INF016 Infrastructure Backup and Archive Service
PLT010 Cloud Services Management and Integration Service
APP001 Approved Commercial-off-the-shelf Products Procurement Service

Underlying Services: OTH001, SME005

Standard Service Support Levels:

Flavours	Availability Target	Service Restoration Period (for P0/P1 incidents)
PLT006-1 Shared Database Hosting	99.9%	8 hours (business)

PLT006-2 Dedicated Database Hosting		
PLT006-2A Stand Alone	98.0%	27 hours (business)
PLT006-2B With High Availability only	99.9%	4 hours (wall clock)
PLT006-2C With Disaster Recovery only	99.0%	8 hours (business)
PLT006-2D With High Availability and Disaster Recovery	99.9%	4 hours (wall clock)
PLT006-3 Oracle Technology Product Licenses	Not Applicable	
PLT006-ENT Enterprise Technology	Not Applicable	
PLT006-STD Standard Technology	Not Applicable	
PLT006-GEN General Technology	Not Applicable	

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Trainings (not covered by service rate):

A3045	Introduction to SQL Language
A3123	Postgre SQL Administration

Service Cost / Price: Please see Service Rates document for standard rates applicable to the service.

N.B. The **Architecture** and **Technology** Flavours must be chosen together as they are complement each other.

- Service Architecture Flavours (PLT006-1, 2A, 2B, 2C, 2D) costs are calculated based on the data size requirement. Service Unit (SU) is #GB.
Service Technology Flavours (PLT006-ENT, STD, GEN) costs are calculated based on the core requirement. Service Unit (SU) is #Core.

PLT008 DevSecOps Service

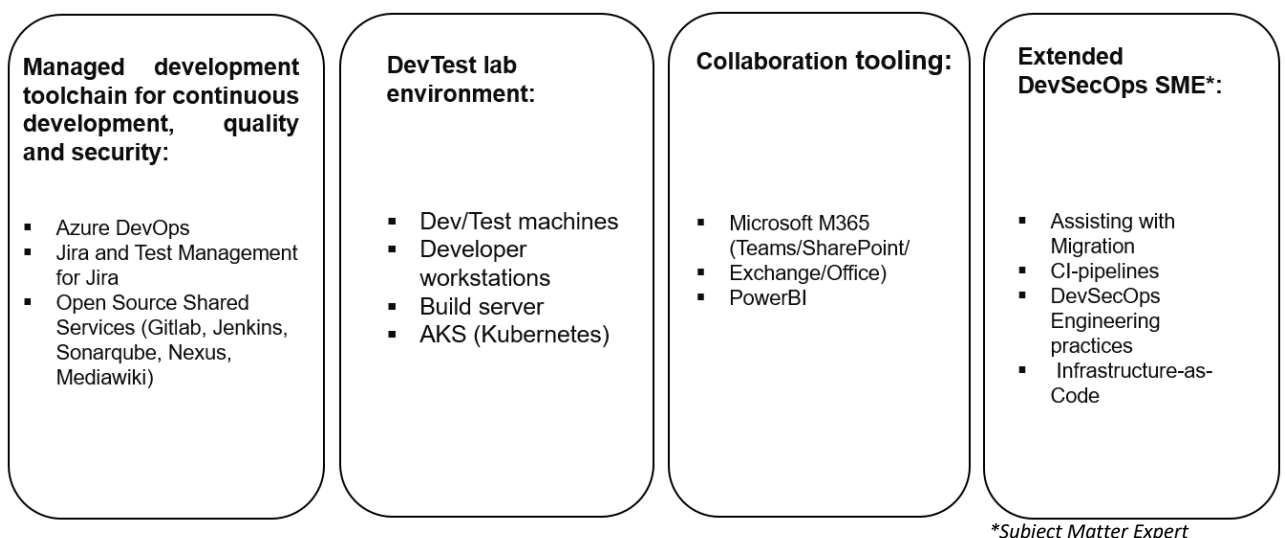
Service ID: PLT008

Service Name: DevSecOps Service

Portfolio Group: Platform Services

Service Description : PLT008 DevSecOps service is available for NCI Agency internal and external customers' needs to manage software application lifecycle.

It consists of a security accredited DevSecOps platform, which enables the NATO Software Factory (NSF) as a space for the collaboration between NCI Agency, Industry, Nations and Academia for development and test activities.



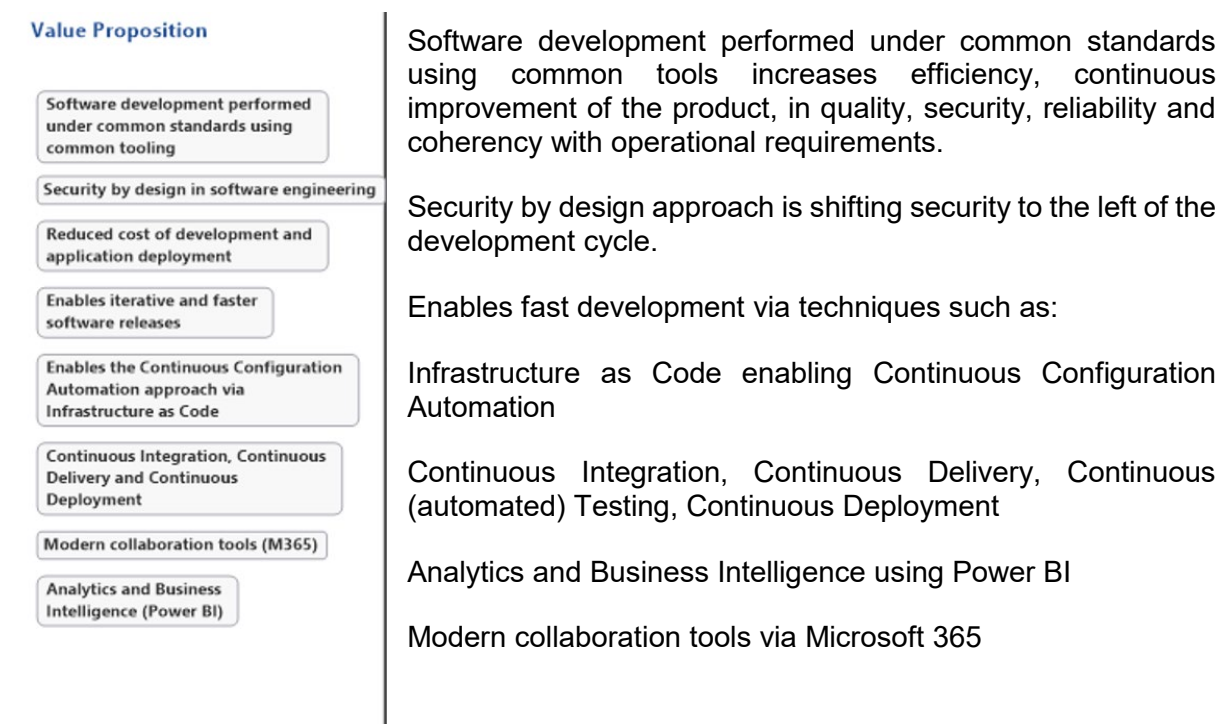
DevSecOps service key activities

PLT008 is available as Platform as a Service (PaaS) in support of the following practices:

- Requirements Management;
- Architecture & Design;
- Agile development;
- Continuous Integration (Build & Test);
- Test Automation;
- Continuous Delivery (Deploy & Release);
- Security By Design;
- Infrastructure as Code (IaC).

Value proposition:

DevSecOps service provides a secure platform, collection of best practices and expertise, tools and modern security habits that increase the ability to securely deliver applications and services at high velocity by closing the gap between development and operations. It aims to shorten the development lifecycle and provide continuous delivery with high quality.



The Service brings several business benefits where:

1. The Agency and NATO stakeholders exploit the Software Factory in which development is performed under common standards using common tooling;
2. It represents mandated PFS in procurements for NSIP;
3. Through self-service cloud provisioning, suppliers working on projects or service adaptation can deploy standard environments for development, testing and regression testing;
4. These environments can be populated with test instances of all services that the component under development consumes;
5. Software development is performed with Security by Design approach taking advantage of automation to perform security policy for:
 - a. Protect Credentials from theft;
 - b. Scan OSS components for vulnerabilities;
 - c. Red-team war games;
 - d. Threat modeling;
 - e. Block lateral movement;

f. Secure and Compliant Pipeline.

The benefits of the Service include:

- Enabled end-to-end traceability from the original operational requirements to the implemented solution components;
- Establish the intended collaboration (technology and practices) with Industry;
- Increased quality of FAS releases through traceability, real-time progress information, ongoing/recurring testing and through feedback loop for production incidents;
- Increased manageability through centralization and automation;
- Enable iterative and faster SW releases (release cadence);
- Better instruments to manage portfolio;
- Better control over IPR;
- Easier onboarding of new staff due to alignment with industry methodologies and best practices;
- Improve the efficient use of valuable resources (Staff, Infrastructure, Funds);
- Enable planned and implemented reuse of SW components;
- Reduced cost of development and application deployment (installations);
- Introduce the approach of Security by Design for software applications.

Service Features:

Access to managed and supported NSF Toolchain: The DevSecOps platform is used as development and testing environments, and it offers a series of tools (NSF Toolchain) based on both Microsoft, and Open Source Stack technology (OSS) ecosystems to ensure coherency with NATO C4ISR Application and Technology architectures. NSF Toolchain is available in Annex A.

DevSecOps SME support: Dedicated support on requestor-specific DevSecOps processes and implementation scenarios such as

- Continuous planning: Agile planning, Thread modelling, Security requirements
- Continuous integration: Test-driven development, shift-left testing, micro-services/container development, static application security scanning, secrets scanning
- Continuous delivery: infrastructure as code, release pipeline, security testing, monitoring, telemetry

Cloud Security Operations activities:

- monitoring,
- detection and response,
- event and incident response,
- continuity of operations,
- threat hunting

using cloud native tools such as:

- Microsoft Sentinel

- Microsoft Defender for Cloud
- Azure and M365 Logging and monitoring
- Various Microsoft Defenders protecting workloads (O365, endpoint, Identity, cloud apps, containers, DevOps etc)
- Azure Active Directory Identity Protection
- Endpoint detection and response (EDR) solution
- Microsoft Purview Compliance Manager

Service Flavours:

The service is available in the following flavours.

1. NSF Standard Profile: Provides access to all NSF services. This is required for most users. Typical use: Developers, Engineers, Testers.
2. NSF Stakeholder Profile: Provides access to NSF Team stakeholders without having to procure a NSF Basic User Profile. The stakeholder will be able to use VPN client to join events such as specific test events, User Acceptance Test (UAT) and Demonstrations.
3. NSF Jira Profile: Limited NSF user profile that only grants access to JIRA. Typical use: Customer representatives (JIRA based projects), JIRA project management (non-software).
4. NSF ADO Profile: Limited NSF user profile that only grants stakeholder access to Azure DevOps (allows access to wiki and work items only). Typical use: Customer representatives (ADO based projects).
5. NSF GitLab Profile: Limited NSF user profile that only grants access to GitLab. Typical use: External collaborators (e.g. partners from NATO nations).
6. For NSF standard profile the following services are available as additional options:
 - a. NATO Trusted Container building service
 - i. Service flavor to consume a centralized pipeline to build trusted application containers
 - ii. Security vulnerability and compliancy assessment using automated scanning tools
 - iii. Promotion to NATO Trusted Container Registry for use of containers on operational networks
 - iv. Security Validator
 1. Based on the findings, mitigations, justifications, and other relevant container characteristics, the Security Validator assigns a container image a trust level and documents any restrictions regarding its deployment
 - b. NATO Trusted Container registry consumption service
 - i. Container platform to consume the NATO Trusted Container Registry on operational networks.
 - ii. Requires a diode to transfer container images from low to high using 1-way diode
 - iii. Centralized high-available container registry on NS
 - c. NSF Managed Endpoint: secured managed baseline for end-user devices accessing NSF resources

- i. Unified endpoint management - cloud based endpoint management, security hardening and compliance management, apps management, content management
- ii. Endpoint Protection Platform - security protection via Microsoft Defender for Endpoint, EDR (endpoint protection and response) and threat hunting integration with NSF Security Operations (SOC)

Available on:

Hybrid, Public Cloud (NU), Private Cloud (NS)

Service prerequisites:

No service prerequisites

Underlying Services: INF046

Standard Service support levels:

		Availability Target	Service Period	Restoration
During hours	Support	99.9 %		2h
Outside hours	Support	99.9 %		Best effort

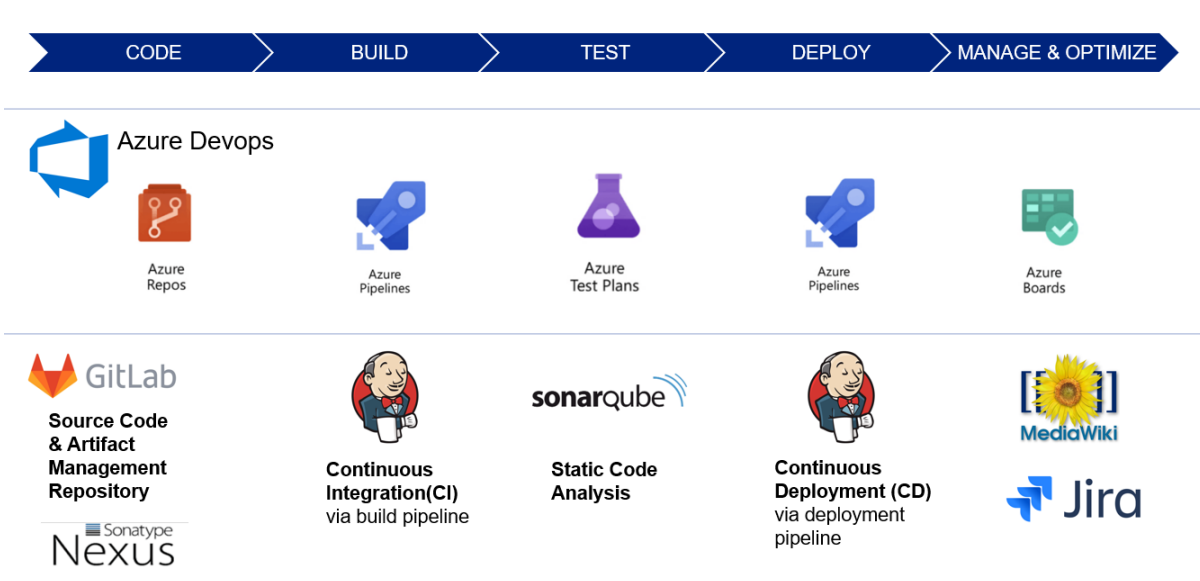
The levels in the table refers to the management and support of the NSF Toolchain. Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. The service Restoration depicts that 70% of reported incidents should be resolved in the specified timeframe.

The service is supported by incident management, service request management and onboarding management processes details of which are available from related Service Delivery Plan and Service Support Package.

Service Cost / Price: For all PLT008 service flavours, there is a fixed license cost per user per month to cover cloud consumption costs for hosting and supporting NSF toolchain. The PLT008 costs and license costs that are part of the NSF user profiles.

Additionally, on top of either one of the flavours, PLT008 SME support can be requested. For this service, there is a fixed labour cost per hour per month to cover the manpower resources responsible to deliver the dedicated SME support.

Annex A. NSF Managed Development Toolchain



Service Assets – Software Descriptions		
Item	Name	Description
1		Kubernetes, or k8s (k, 8 characters), is an open source platform that automates Oracle Linux container operations. It eliminates many of the manual processes involved in deploying and scaling containerized applications. In other words, It is possible to cluster together groups of hosts running Oracle Linux containers, and Kubernetes helps easily and efficiently manage those clusters. These clusters can span hosts across public, private, or hybrid clouds. For this reason, Kubernetes is an ideal platform for hosting cloud-native applications that require rapid scaling, like real-time data streaming through Apache Kafka.
2		GitLab is a Git-based platform that integrates a great number of essential tools for software development and deployment, and project management: • Hosting code in repositories with version control. • Reviewing code in Merge Requests with live-preview changes per branch with Review Apps. • Deploying personal and professional static websites with GitLab Pages. • Tracking the development lifecycle by using GitLab Cycle Analytics.

Service Assets – Software Descriptions		
Item	Name	Description
3		Jenkins is a self-contained, open source automation server which can be used to automate all sorts of tasks related to building, testing, and delivering or deploying software. It can be used with large variety of build systems, such as Maven, Gradle, NPM and yarn. It can be used for simple build tasks but also for complex multistage CI pipelines.
4		Jira is a family of products built to help all types of teams manage their work. Jira offers several products and deployment options that are purpose-built for Software, IT, Business, Ops teams, and more. JIRA Software allow to plan, track and release world-class software. • Bug tracking • Project management • Product management • Process management • Task management • Software development • Agile software development • Test Management
5		SonarQube (formerly Sonar) is an open-source platform developed by SonarSource for continuous inspection of code quality to perform automatic reviews with static analysis of code to detect bugs, code smells, and security vulnerabilities on 20+ programming languages. SonarQube offers reports on duplicated code, coding standards, unit tests, code coverage, code complexity, comments, bugs, and security vulnerabilities.
6		Manage and store components from dev through delivery, build artifacts, binaries, containers, assemblies, and finished goods (releases and release candidates) in one central location, including intelligent staging and release functionality. Understand component security, license, and quality issues. Store and distribute Maven/Java, npm, NuGet, RubyGems, P2, OBR, APT and YUM and more. Nexus IQ and Firewall prevent vulnerable and noncompliant components from entering the software supply chain, based on governance policies. When new components are downloaded, Firewall scans every new package against a set of organization-defined policies. Any component or dependency that violates one of these policies is then blocked from the repository.

Service Assets – Software Descriptions		
Item	Name	Description
7	 AZURE DEVOPS	Azure DevOps Services provides development collaboration tools including high-performance pipelines, free private GIT repositories, configurable Kanban boards, and extensive automated and continuous testing capabilities. It includes: • Azure Boards • Azure Pipelines • Azure Repos • Azure Test Plans • Azure Artifacts • Extensions Marketplace
8	 MediaWiki	The MediaWiki software is used by tens of thousands of websites and thousands of companies and organizations. MediaWiki helps you collect and organize knowledge and make it available to people. It's multilingual, free and open, extensible, customizable, reliable, and free of charge.

PLT009 Electronic Definitive Media Library (EDML) Service

Service ID: PLT009

Service Name: EDML Service

Portfolio Group: Platform Services

Service Description: Electronic Definitive Media Library (EDML) service is available to customers to meet the demand for media delivery. Example of media are COTS SW, NATO FAS, artefacts, graphics and documentation. The service is available from the public cloud, Microsoft Azure.

Value proposition: EDML allows exchanging data in a more flexible and secure way, with reduced “Mean Time To Resolve” (MTTR) while keeping control over access and delivery in today’s high standards of secure access.

Service Features: The Electronic Definitive Media Library provides a secure one-stop-shop for NATO software and media, accessible from anywhere in the world. It offers a number of specific benefits including user registration and controlled user access, public key encryption and access logging and auditing.

Service Flavours:

1. **NATO App Store.** Allows NATO Nations and NATO Partners, which have signed a NST Licence agreement with NATO to download NATO software tools used for testing, evaluation and operational purposes.
2. **Multi-tenant Media Delivery (SaaS¹).** Instances of EDML enabling:
 - Data segregation between EDML instances
 - RBAC access mode with tenant administration accountability to customers whereas main root administration is ensured by the service provider
 - Upload of media via the Uploader App, which encrypts the media before the move to public cloud service provider datacentre;
 - Visibility and transparency over service cost consumption from the service provider;
 - Access the EDML Decrypter App required for the download of media.

Available on:

Public Cloud (NU)

Service Prerequisites:

None

Underlying Services: PLT008

Standard Service support levels:

¹ In a nutshell it means that I can have different EDMLs for different cases but that do more or less the same thing: uploading and downloading media.

Perfective, adaptive, and corrective maintenance, as well as service support and cloud resources are included.

		Availability ¹ Target	Service Period	Restoration
During hours	Support	99.9 %		2h
Outside hours	Support	99.9 %		Best effort

The levels in the table refers to the management and support of the EDML tenants. Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. The service Restoration depicts that 70% of reported incidents should be resolved in the specified timeframe.

The service is supported by incident management, service request management and on-boarding management processes details of which are available from related Service Delivery Plan and Service Support Package.

Service Cost / Price: The unit of measure of NATO App Store service flavour is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. The unit of measure for the **Multi-tenant Media Delivery (SaaS)** flavour is per tenant per year with cost break as per Annex A.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

PLT010 Cloud Services Management and Integration (CSMI) Service

Service ID: PLT010

Service Name: Cloud Services Management and Integration Service

Service Type: Enabling

Portfolio Group: Platform Services

Service Description: PLT010 enables public cloud-based services and facilitates a scalable CIS environment for NCI Agency's internal and external customers over the public internet. It operates across multiple security-accredited cloud environments and offers a robust suite of services that leverage the benefits of the public cloud, including scalability, flexibility, enhanced security, and high availability.

Value proposition: The Service offers the following benefits to cloud-based services or flavours:

- Scalability and Flexibility in the lifecycle of cloud resources to meet evolving business needs.
- Security and compliance with NOS and NCSC security policies for public cloud environments;
- Reliability and High availability provided by the cloud provider, based on agreed KPIs, to minimize downtime and ensure uninterrupted access to cloud resources.
- Monitoring and Performance Optimization to effectively manage and control resource consumption.
- Integration with Enterprise Identity Access Management (WPS002) for secure access via Multi Factor Authentication.
- Vendor Management to liaise with relevant Cloud Service Providers, assess service levels, and ensure compliance with agreed-upon terms, conditions and KPIs.

Service Features:

- **Cloud Service Management and Governance**, including cloud cost management, tenant and subscription management;
- **Identity and Access Management**, including account management, conditional access, permissions and policies (through WPS002- Enterprise IDAM Service);
- **Cloud Resource Management**, including networks, subnets, VPNs, compute and storage, backups operations, IaaS, PaaS and SaaS offering of cloud provider;
- **Scalability and Flexibility**, in terms of deploying, managing and scaling resources to accommodate changing workloads and business requirements.
- **Monitoring and Performance**, including comprehensive monitoring capabilities to track the performance, availability and health of cloud resources;
- **Cloud Security & Compliance**, including hardening of the resources offered by cloud provider, as well as security monitoring and compliance;

- **Integration of the cloud-based services** into the existing Service Management and Control (SMC) processes, as well as the existing resources and services;
- **Shared Foundation** with below capabilities:
 - Capacity management (tenant wide):
 - Controlling, monitoring and optimizing resources usage to keep the cost in agreed limits,
 - Provisioning of resources, implementing and maintaining the templates (200+ products offered by Cloud provider),
 - Setting and monitoring the configured metrics like performance, resources consumption, security, availability.
 - Cost management / FinOPS (tenant wide):
 - Optimizing the cost of each subscription to stay in the agreed financial limits,
 - Migrating the resources between different groups or locations to reduce the cost or increase the saving,
 - Monitoring and controlling the cost of shared foundation service to lower the financial implications,
 - Accreditation & documentation (tenant wide & assisting subscriptions):
 - Supporting accreditation and development of document package for shared foundation, as well as subscriptions.
 - Registering any design and architecture changes on tenant level into the respective CIS Description.
 - Reviewing, updating SecOps, SOPs, SOIs and providing feedbacks for respective contracts.
 - Integration (tenant wide & assisting subscriptions):
 - Enabling platform for common and managed services as “shared foundation” at tenant level,
 - Delivering the underlying, secure and accredited shared foundation for each subscriptions,
 - Integration of new resources with shared foundation to achieve standards and to ensure governance at tenant level.
 - Enabling and configuring built-in tools for tuning, securing, logging, alerting and notification in tenant and subscriptions,
 - Automation of provisioning and configuration of resources (IaC),
 - Lifecycle management of APIs and interconnectors,
 - Providing Level-3 support for subscription, and Level-2 on tenant level,
 - Tenant management:
 - Governance of the tenant, and managing tenant level resources, including global administration,
 - Managing and controlling the global level permissions, rights of the tenants,
 - Managing lifecycle of subscriptions; assignment of customer and resources to the subscription,
 - Tagging all resources for empowering fair costing and charging the service,
 - Policies (tenant wide):
 - Ensuring the compliancy of the latest NATO regulations and best practices.
 - Implementation, monitoring and control of applied policies, like conditional access, allowed locations for resource deployments, taxonomic tag enforcement, diagnostic logs and analysis.
 - Remediation of resources non-compliant with policies.

Service Flavours: The Service is available in two flavours:

1- MARIE (Maritime Information Exchange): MARIE is a dedicated cloud environment for HQ MARCOM to enable an information exchange platform.

A- Starter pack: is required to enable and deliver the initial setup for the requested capacity. The cost of this flavour covers the first 50 users of the platform. The unit measure for this flavour is “1”.

B- Additional users: This flavour is for additional users after the first 50 that come with “Starter pack”. The unit measure for this flavour is “per User”.

2- Customized Solutions: These capabilities cannot be used as-is directly from the cloud provider and require a high level of customization. They are tailored to meet specific business or operational needs that go beyond the standard offerings of public cloud services. As such, they are not managed by the cloud provider. The total cost includes the value of the assigned resources (via AWS or Azure credits), as well as the cost of shared foundation and the secure platform that supports them. Due to the complexity and level of customization involved, these solutions require a greater amount of workforce for ongoing maintenance and operations.

The unit of measure is defined as “per Credit” to maintain consistency with the service provider’s pricing model.

3- Out of Box Solutions: This service flavour is intended for standardized, ready-to-use solutions that require little to no customization. The capabilities are fully managed by the cloud provider and typically include services such as managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services are provisioned and maintained by the provider, significantly reducing the operational burden on internal teams. Due to their managed nature, these solutions require minimal workforce for ongoing maintenance, monitoring, and operations. They are ideal for organizations seeking efficiency, speed of deployment, and reduced complexity in managing cloud-based services. The total cost covers both the assigned cloud resources (provided through AWS or Azure credits) and the underlying shared functions and secure platform that support the service delivery. This ensures that all technical, security, and operational aspects are included in a single, predictable cost structure.

The unit of measure is defined as “per Credit”, consistent with the cloud provider’s pricing model to ensure transparency and alignment with actual resource usage.

4- NPCL (NATO Public Cloud): NPCL is a dedicated environment built on MS Azure to host and enable the NU Public Access Network (PAN).

The unit of measure is defined as “per Credit” to align with the service provider’s cost model. The required number of credits for the PLT010 service matches the amount requested by the service provider. The cost of the service flavour includes the service provider’s base cost for IaaS and PaaS offerings, along with additional charges for support, shared foundation services, staging, and advanced security.

Available on:

Public Cloud at NATO Unclassified level.

Service Prerequisites:

WPS002 Enterprise Identity and Access Management Service

Standard Service Support Levels:

	Availability Target	Service Period	Restoration
Support hours	Based on KPIs ¹	Based on KPIs ¹	

Service Cost / Price:

Service ID		Unit of Measure
PLT010 – 1A	MARIE Starter pack (incl. first 50 users)	1
PLT010 – 1B	MARIE Additional users	Per user
PLT010 – 2	Customized Solutions	Per Credit
PLT010 – 3	Out of Box Solutions	Per Credit
PLT010 – 4	NPCL (NATO Public Cloud)	Per Credit

¹ Depending on the contract conditions, KPIs with Cloud Provider and/or Customer.

PLT011 Cloud Application Access (CloudApp) Service

Service ID: PLT011

Service Name: Cloud Application Access (CloudApp) Service

Portfolio Group: Platform service

Service Description: The Cloud Application Access Service provides users with the possibility to access applications in the NATO Datacentre through the use of a local web browser. The Cloud Application Access Service provides a simple web page containing icons for the applications the user can access. A centralised application provisioning allows a single point of management for the application baseline and user authorisation.

Value Proposition: The Cloud Application Access Service allows the user to securely use an application published in the NATO Datacentre from any IP connected device with a web browser. This service may be used to allow the user from the NATO Secret (NS) network to access published applications on a Mission Secret (MS) domain in the NATO datacentre (Mission Information Room, MIR) without the need for a MS workstation.

Service Features: The service features include secure web access to a web page that lists a selection of icons for every published application for each particular user. By accessing this published application, a local session (in the datacentre) starts under the credentials entered as part of the web page logon.

As the session and application data is running in the NATO datacentre, the performance for each user is identical (depending on the type of network access).

Usage, metering, and performance measures are being recorded and may be shared with the customer representative.

Service Request: Once the service is contracted by SSP/SLA, the service can be requested through an ITSM request for a single or a group of users.

As the Cloud Application Access Service needs coordination with the dependent services (IaaS/Identity) and depending services (CES/COI applications) a Service Delivery Manager (SDM) is available for close coordination with the customer. The SDM will be the point of contact for coordination planning, problem management and performance reporting which will be critical in particular as part of NRF exercises

Service Flavours:

MIR Cloud: Specific flavour of Cloud Application Access Service that allows access to MS published applications from the NS network

NS/NU Cloud: Specific flavour of Cloud Application Access Service that allows access to NS/NU published applications from the same NS/NU network. Note that the client device from which the application is accessed does not need to be managed by NCIA (f.e. BICES)

Available on: NU (PAN), MS (NRF, NMI, Op Sea Guardian), NS (AIS)

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side)

NDW003 Personal Workspace- Managed Device Service

WPS002 Enterprise Identity Access Management Service, the user requires a user account for the domain on which the application is published;

WPS003 Enterprise User License Service, or otherwise licensed relevant Microsoft office software;

INF004 Infrastructure Virtualization service and INF005 Infrastructure Integration Service, as the Cloud Application Access Service needs to be hosted on the NATO Data centre infrastructure;

INF007 Infrastructure Storage Service, the user requires a personal profile storage space (minimum 3 GB on default) to be able to store user profile files.

Underlying Services: OTH001, PLT008, SME005

Standard Service Support Levels:

	Service Flavour	Availability target during support hours	Availability target out of support hours
Level 1	MIR Cloud	99.9%	99.5%
Level 2	NU/NS Cloud	99.5%	99.0%
	Service Flavour	Restoration period during support hours	Restoration period out of support hours
Level 1	MIR Cloud	1 hour	4 hours
Level 2	NU/NS Cloud	1 hours	4 hours

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Concurrent User (CCU), with a minimum number of 10 CCUs required to establish the Service on an existing CloudApp Platform (100 CCUs are required for a dedicated Platform). The price details available in the Service Rates document.



PLT012 Maritime Command and Control Platform (MARC2P) Service

This service has moved to INF056 Deployable CIS Nodes for Maritime Based Users (MBU) and has been reclassified as INF057 Maritime Command and Control Platform (MARC2P) Service.

PLT013 NATO Integrated Secure Platform (NISP) Service

Service ID: PLT013 (old ID: APP051)

Service Name: NATO Integrated Secure Platform (NISP) Service

Portfolio Group: Platform Service

Service Description: The NATO Integrated Secure Platform (NISP) has been developed as a tool to work alongside the Solaris operating system (OS), simplifying the Solaris installation and common system administration tasks. NISP provides the means for implementing a networked platform, open to a range of applications, which ensures site installations are easier to maintain and can be supported centrally. NISP has become the standardised general purpose system configuration tool, suitable for all AirC2 applications supported by the NCI Agency.

Value proposition: NISP realizes the value at the user side by standardizing Solaris and Oracle Linux based Operating System platform installation and configuration while securing the installation in accordance with Cyber Defence mandated CIS security settings.

Service Features: The NISP Service offers the user:

- Simplified installation and maintenance of Solaris and Oracle Linux based Operating System Platform,
- Easing the tasks of the system administrator by providing a rich set of scripts for installation and administration,
- Securing these OS platforms by applying a pre-configured set-up as required for NATO networks,
- Providing security and OS patches either periodically, on demand or on request by the user,
- Standardize the Solaris and Oracle Linux based installations and configurations for easing system platform support and troubleshooting,
- Comprehensive documentation for system installation, configuration and administration,
- Supports SPARC for Solaris as well as Intel x86 based hardware for Solaris and Oracle Linux.

Service Flavours: NISP flavours that the customers can choose from are:

- Full NISP Software Baseline Maintenance and In-Service-Support (ISS) for NCS sites,
 - This service flavour is NATO common funded and includes maintenance of the NATO NISP single SW baseline which is a pre-requisite for all other service flavours which are offered through the service catalogue.
- Stand-alone server or client installations,
- Fully integrated, networked solution including NISP client and server as well as windows network integration if required.

Available on:

NATO Unclassified

NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

INF004 - Infrastructure Virtualization Services to provide the server instance (either physical or virtual) on which a NISP server can be deployed.

Alternatively to INF004, NISP can be deployed on server and client hardware or virtual infrastructure compatible to install and run Solaris or Oracle Linux.

NISP for Solaris instances requires a license for the Solaris operating system IAW Oracle license terms and conditions.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

- Belgium +32 65 44 3177
- Netherlands +31 70 374 3177
- Italy +39 081 721 3177
- Germany +49 282 4978 3177
- USA +1 757 747 3177
- For NATO HQ +32 02 707 5858

Service Requests:

To request the PLT013- NISP service, please complete the Customer Request Form and contact NCI Agency through the submit function included in the form following the link below.

https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

NISP functional unit	Service Level Target (availability)	Performance Thresholds
Client installation	99.5%	15" (start-up) 30" (re-start)
Server installation	99.5%	10' (start-up) 15' (shut-down)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1000	Combined NISP ICC System Administrator (CNIC)
A1006	NISP System Administrator

Service Cost / Price: The unit of measure for all Service Flavours is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit
PLT013	NATO Integrated Secure Platform (NISP) Service	NISP software baseline maintenance and In Service Support (ISS) for NCS sites	1
PLT013	NATO Integrated Secure Platform (NISP) Service	Stand-alone Server or Client installation	1
PLT013	NATO Integrated Secure Platform (NISP) Service	Server and client installation integrated into existing networks	1

PLT014 Integration Tests Platform Service

Service ID: PLT014

Service Name: Integration Tests Platform Service

Portfolio Group: Platform Services

Service Description: The Service provides a production-like environment, tools and services based on the NATO Software Factory that enables running the mandatory integration tests for all those FAS or applications that have dependencies or interactions with other applications or core services, on the basis of automation to the maximum extent possible. In addition, this service provides the Integration testing subject matter expertise (SME) in charge of executing test plan and test cases mandatory for the contractual obligation of contractors during project implementation and during the integration activities required during the O&M of application services.

Value proposition: The Service offers the following benefits to projects by using cloud computing:

- Takes advantage of cloud service provisioning, to rapidly and cost effectively deploy readily available production-like infrastructure environments and virtual machine for applications, only available the time needed for running integration tests.
- Increased manageability through self-service, centralization, and automation;
- PLT014 is offered as PFS (Purchaser Furnished Service) for integration testing for NATO applications under procurement;
- Improve the efficient use of valuable resources (Staff, Infrastructure, Funds);
- Direct access to DevTest environments in the NATO Software Factory DevSecOps platform, taking advantage of rapid installation of relevant application releases.
- PLT014 is part of NSF services, with security accreditation granted by Security Accreditation Authorities
- Integration test toolchain support and import of test plan and test cases designed for the specific integration tests.
- Coherent with NATO Software Factory architecture and technical compliance;

Service Features:

Automated Infrastructure Provisioning, including AD infrastructure, official GPOs and security settings, VM management, patching, antivirus and related services via Continuous Integration (CI) pipeline.

Application Provisioning; deployment and configuration of applications in the infrastructure, with official releases and configuration instructions provided by application service delivery managers.

Management of toolset; Test management tooling with support from test SMEs

PLT014 FAS Catalogue: lists all core services and FAS available on PLT014 and provides for each service configuration details, version information, service end points, and points of contact.

Service Flavours: The Service is available as a single flavour.

Available on:

Hybrid and Public cloud at NATO Unclassified level that may carry administrative markings

Service Prerequisites:

PLT008 DevSecOps platform.

Standard Service Support Levels:

		Availability Target	Service Restoration Period
During hours	Support	99.9 %	2 hours
Outside hours	Support	99.9 %	Best Effort

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The cost of the service comprises a fixed cost portion and a variable cost portion:

The fixed cost portion is mandatory for the service to exist. It is not attributable to a single project using the platform. It covers the costs required to operate and maintain the platform. It includes the manpower and expenses required for:

- Support
- Onboarding
- Patching
- Service updates (Core Services)
- Self-service portal
- Maintenance of PLT014 available services catalogue
- Service improvements

The dynamic costs are charged to each individual project based on the actual usage of the platform by that project. These costs include the Azure consumption (storage and compute) and the optionally procured Test SME support. The Azure consumption will be charged against each project's balance of Azure credits (as procured through PLT008). The Test SME support will have to be procured in advance.

PLT015 CQO Reference Platform Service

Service ID: PLT015

Service Name: CQO Reference Platform Service

Service Type: Customer facing, Supporting and Enabling

Portfolio Group: Platform Service

Service Description: The CQO Reference Platform Service provide environments and tools in support of Interoperability testing and formal V&V for internal and external projects.

Value Proposition: CQO Reference Platform Service provides a reference infrastructure and/or Interoperability testing infrastructure to the projects, including international entities. It facilitates activities for testing, demonstration and exercises. Since the CQO Reference Platform Service is a shared infrastructure with multitude of subscribers and users and associated economies of scale, it saves cost, increases quality and lowers participants' risk by providing a standard and accurate reflection of the production environment. The CQO Reference Platform Service is complementing the CQO test services [SME002]. It provides a platform and virtual machines used in testing those products that cannot be tested in NSF. It can also be used as a stand-alone or supporting service in other projects and programmes. CQO Platform Reference Service offers an agile and fully service based non-operational infrastructure, and operates at up to a Secret releasable accreditation level. CQO Platform Reference Service provides common framework, well-defined processes, security procedures and agreed technical standards.

Service Features:

service			Resources consumed															
				IaaS & PaaS (Mandatory - new IaaS)	IaaS & PaaS (Mandatory - standard IaaS)													
						SMALL VM (2/4/50)	MEDIUM VM (4/16/100)	M-LARGE VM (8/32/200)	LARGE VM (12/48/300)	X-LARGE VM (16/64/500)	Dedicated VDI VM	Additional Storage Capacity (1.8 TB HDD)	Additional RAM memory (32 GB)	Thin Client Provisioning & Lab Space	total vCPU	total RAM (GB)	total storage (GB)	Project management costs
Project env	New project env	INV labor		€ 98.98	€ 87.59	€ 52.50	€ 100.00	€ 195.00	€ 290.00	€ 385.00	€ 210.00	€ 50.00	€ 10.00	€ 15.00				
RefEnv 'NU'	☐	FALSE		0	0	€ 32.50	€ 40.00	€ 55.00	€ 70.00	€ 85.00	€ 100.00	€ 0.00	€ 0.00	€ 75.00	0	0	0	€ 12,191.84
RefEnv 'PINK'	☐	FALSE		0	0										0	0	0	
RefEnv 'RED'	☐	FALSE		0	0										0	0	0	
	☐	SUM		0	0	0	0	0	0	0	0	0	0	0	0	0	0	

Service Flavours: The service will be adapted to the customers resource and hosting requirements and classification/releasability level.

The Test Tool Sub-Service will be adapted to the size of the user community.

Available on: NS Ref., NU-IVV-Ref, and applicable CFBLNet enclaves (e.g. CUE, RED, PINK). NU Environment accessible through Reach capability.

Service Prerequisites: NCIA subscribers: Technical Work Area (TWA) / Facility space with (diskless) workstation and connected to the CQO service infrastructure as required.

Standard Service Support Levels:

Service Availability Target: During Initiates, depend on the underpinning environments and underpinning contracts though 99 % is a minimum target.

Service Restoration: Service response time during business hours 9 Business hours. Where the service is deemed unavailable, the service restoration period for a critical incident is 18 Business hours. (Better can be negotiated)

N.B. Service is a non-operational service as such will have a lower resilience and availability.

Service Cost / Price: The overall services cost is calculated on a case-by-case basis for the subscriber of the shared service. The calculation principle is summarised in the table under service features section.

This page is left blank intentionally

Subject Matter Expertise (SME) Services

SME002 Independent Verification and Validation for A2SL Service

Service retired and replaced by TST001.



SME003 Interoperability Verification and Validation Service

Service retired and replaced by TST002.

SME004 Provision of Subject Matter Expertise for the Federated Mission Networking (FMN) Framework

Service retired and replaced by FMN001. Service Description for FMN001 is in Appendix 2 – Non-Costed Customer Services.

SME005.1 Acquisition Life Cycle Cost Estimating (LCCE) Service

Service Retired



SME005.2 Acquisition Software Intensive Project (SIP) Cost Estimating Service

Service retired.

SME005.3 Acquisition Cost Analysis (CA) Service

Service retired.

SME005.4 Acquisition Miscellaneous Cost Estimating & Analysis (MCEA) Service

Service retired.



SME007 Operational Application Support Service

Service retired and replaced by APP113.

SME008 Maritime Operational CIS Deployment and Recovery Service (MARCOM)¹

Service ID: SME008

Service Name: Maritime Operational CIS Deployment and Recovery Service

Portfolio Group: Subject Matter Expertise Services

Service Description: This service provides Planning, Deployment, Implementation, Training and Recovery, of CIS services. These services may include all or some of the following: Maritime Command and Control Platform (MARC2P) Service (INF057), SEMARCIS service (INF044) & Tactical Satellite (TACSAT) service (INF040). These services can be provided to and from customer designated location(s) within SACEUR's Joint Operational Area (JOA).

Value proposition: This service enables the customer to maintain a level of operational command and control when established on board a designated vessel or at a specified static location.

Service Features:

Planning: This requires in-depth coordination with the customer, any nominated additional points of contact, the designated Naval vessel, and if necessary, the Host Nation (HN) of the oncoming vessel. The planning process also includes a site survey of the oncoming vessel 90 days ahead of time for full operational handovers. A site survey may be required for all other activities. This is critical to facilitate a common understanding of the full scope of the upcoming activity, and to advise the HN designated vessel in their preparation to take on the CIS services.

Deployment: Includes the requested CIS service(s) equipment to be forward deployed to a designated Naval vessel (or static location) for installation.

Implementation: Includes the installation, configuration, and commissioning of requested CIS service(s). Equipment is installed on the identified Naval vessel (or static location), and End-to-End (E2E) configuration is completed utilizing remote support from various NCI Agency service areas. All CIS Services are tested on site and commissioned when considered operational and agreed with the customer on site.

Training:

Limited training is provided on site during implementation to designated staff. This includes basic administrator training to facilitate a common understanding of CIS operations, standard operating procedures (SOPs), and basic troubleshooting. This does NOT include in-depth Functional Application Services (FAS) training, as there is an assumed prerequisite knowledge of each of the FAS's deployed.

Recovery: Where requested, CIS service(s) equipment will be decommissioned (ceasing services), de-installed, and then subsequently recovered to NCI Agency

¹ Outside of MARCOM this Service can be requested on a case by case basis via a CRF. The cost for the service may be different from the catalogue as it will depend on the requirement written in the CRF.

control. At times the same equipment may be immediately re-allocated for additional tasking.

Service Flavours:

SME008-1A Maritime Operational CIS Deployment/Recovery Service – Collocated Major Handover: Includes removal of the INF057-1 Single Domain (NS) MAR C2P service, TACSAT (if installed), and/or SEMARCIS/SEMARCOM (if installed) CIS equipment from one identified Naval vessel, immediately followed by installation on another identified Naval vessel at the same designated port of call.

SME008-1B: Maritime Operational CIS Deployment/Recovery Service – Collocated Major Handover: Includes removal of INF057-2 Dual Domain (NS & NU) MAR C2P service, TACSAT (if installed), and/or SEMARCIS/SEMARCOM (if installed) CIS equipment from one identified Naval vessel, immediately followed by installation on another identified Naval vessel at the same designated port of call.

SME008-2A Maritime Operational CIS Deployment/Recovery Service – Non-Collocated Major Handover: Includes removal of the INF057-1 Single Domain (NS) MAR C2P service, TACSAT (if installed), and/or SEMARCIS/SEMARCOM (if installed) CIS equipment from one identified Naval vessel at one designated location, shipment of CIS equipment (via Northwood if required), and subsequent additional travel to a different location for installation on another identified Naval vessel at that separate location.

SME008-2B: Maritime Operational CIS Deployment/Recovery Service – Non-Collocated Major Handover: Includes removal of INF057-2 Dual Domain (NS & NU) MAR C2P service TACSAT (if installed), and/or SEMARCIS/SEMARCOM (if installed) CIS equipment from one identified Naval vessel at one designated location, shipment of CIS equipment (via Northwood if required), and subsequent additional travel to a different location for installation on another identified Naval vessel at that separate location.

SME008-4 Maritime Operational CIS Deployment/Recovery Service – SEMARCIS Deployment / Recovery (DR): Includes deployment and implementation of a SEMARCIS capability on an identified vessel at a designated location and then the subsequent recovery of the SEMARCIS equipment from that vessel at a later date and designated location (may be the same or different from the installation location).

SME008-5 Maritime Operational CIS Deployment/Recovery Service – Tactical Satellite (TACSAT) Deployment / Recovery (DR): Includes deployment and implementation of a TACSAT capability on an identified vessel at a designated location and then the subsequent recovery of the TACSAT equipment from that vessel at a later date and designated location (may be the same or different from the installation location).

Available on:

NATO Secret
Mission Secret
NATO Unclassified

Non-Secure

Service prerequisites:

All service requests must be funded prior to deployment and implementation. This may include support provided under an existing agreement (SLA/SSP) or through funding via the Customer Request (CRF) process.

It is the Customer's responsibility to ensure compliance with the Minimum Military Requirements (MMR) for CIS as stipulated in the MC0195 prior to implementation. The customer is to ensure that the identified Naval vessel has the technical capabilities to support the CIS services (i.e. sufficient bandwidth, National connectivity, authority to install and/or connect to National systems, etc.).

An IT Service Request (ITSM) Change Request Form (CRQ) is required for each requested activity and must include all tasking requirements, POCs, dates and location(s). CRQs are to be submitted as per the schedule below. In exceptional circumstances, this may be shorter, but this will require the customer to accept additional risk of the operational capability of their identified vessels.

- For SME008-1A & 1B and for SME008-2A & 2B a CRQ is required 120 days prior to date of handover.
- For SME008-4 & 5 a CRQ is required 30 days prior to date of activity.

The Customer is to facilitate agreed support for NCIA with the identified Naval vessels at agreed dates and location for implementation. This includes access to the base location, the Naval vessel(s) and coordinating local support on site (i.e. service crane, HN ship support).

A Customer Staff POC is requested to accompany the CSU team onsite during any installation activity. The customer must ensure that all information required to plan the workforce and logistics is provided in line with the time lines above (120 days & 30 Days). Out with these time lines NICA cannot guarantee the workforce required to deploy, and there may be additional cost for shipping (Red Star) to ensure delivery of assets to meet MARCOMs requirements.

The Customer is responsible for accepting, signing for and maintaining accountability of all CIS hardware after implementation until they are formally recovered by NCIA. Any loss of or damage to any CIS equipment may incur additional cost.

The Customer is responsible for ensuring the provision of cryptographic material in order to enable secure communications during operation of the deployed CIS, after implementation.

The customer is responsible for ensuring that all staff, that will utilise the equipment and Functional Application Services on board, are trained to the required standard to be able to participate during the deployment.

Delivery of this service is dependent on allocation of CIS equipment from designated account holders or the customer holding these resources. It is the Customer's responsibility to ensure that the requested resource is available.

Standard Service support levels:

The Service is available at any point in the calendar year in line with the perquisites above.

There is a maximum concurrency of two Deployment / Recovery activities at any time to include travel to/from locations. Any additional concurrent requests will only be considered by exception and on a case by case basis manner.

Service Cost / Price: The unit of measure for the Service is per instance of service flavour requested. For price information, see the Service Rates document.

Service Performance Targets:

Implementation completed by required date for Service Change Requests received with sufficient notice (timelines specified above) and meeting all prerequisites: 95%

Time to complete:

SME008-1. 4 days total.

SME008-2. 5 days total: 4 days for implementation; 1 day for recovery.

SME008-4. 3 days total: 2 days for implementation; 1 day for recovery.

SME008-5. 3 days total: 2 days for implementation; 1 day for recovery.



SME009 Provision of Subject Matter Expertise to support NCS as an Affiliate to Federated Mission Networking (FMN)

Service retired and replaced by FMN002. Service Description for FMN002 is in Appendix 2 – Non-Costed Customer Service



SME010 ACP127 Message Operator Service

Service retired and become flavor under APP029.



SME012 VeVA CIAV Support

Service Retired and replaced by TST002.



This page is left blank intentionally



Testing Services

TST001 Independent Testing Service

Service ID: TST001

Service Name: Independent Testing for Service

Portfolio Group: Testing Services

Service Description: The Independent Testing Service provides a consistent and independent way of verifying and validating products and systems.

The Technical and Implementation Directive on CIS Security (AC/322-D/0048-REV3) provides the minimum set of security measures required to be applied for the protection of NATO classified and non-classified information and the handling CIS. Among those and addressed by this service are:

- A configuration change control process validates, tests, documents and approves all changes to the CIS. The CISP tests software and firmware updates before installation.
- A separate test environment is used to assess new or changed capabilities before introducing them to the operational CIS.

Value proposition:

This service will cover the independent testing required to provide objective evidence that the software or system under test is of satisfactory quality and meets customer, technical and security requirements.

The Agency Approved Software List (A2SL) process is the configuration change control process in place for NS and NU NCI Agency managed networks. This is covered by the 'ACO' Service flavour. It is expected that new projects delivering software to be deployed in NCI Managed Networks will include the initial entry as part of activities in scope of the project, and as such initial entries are out of scope of the 'ACO' service flavour.

Additionally, nations may use the A2SL to inform their CIS Baseline or have other national processes to perform configuration change control on their CIS Baseline. Both may require testing services to fulfil their compliance to AC/322-D/0048-REV3. This is covered by the 'Others' service flavour.

Service Features:

- **Scope Evaluation and Assessment** : This package contains the effort required to manage the service, attend the relevant Change Management Boards (CAB), review all CRQs for A2SL and evaluate the type of testing required for the given CRQ.
- **CQO Reference Platform Service** : This package contains the effort required to maintain the environments to support all testing activities as outlined in this service description. This includes regular maintenance and upgrades, including license management, patching, security configuration and continuous alignment of the reference environment to the operational environments.
- **Testing:** The following activities are costed in each of the test types:

- CRQ management and assessment
- Drafting Test Plan and Test Cases
- Perform Test Readiness Review
- Prepare Test Environment
- Execute Tests
- Drafting Test Report
- Drafting System Administration Notes
- Perform Software Test Review
- Set up, maintenance, updates and clean up of Test Environment

Service Flavors:

- **TST001-1 Operating Systems Testing:**

This package will consist of the effort required to test new operating systems and new versions of approved operating systems in order to integrate it in the NATO Environment.

Scope will include:

- Compatibility with the existing NATO environment.
- Correct functioning of the operating system under NATO security settings and security mechanisms.

- **TST001-2 Patch Testing:**

This package will consist of the monthly effort required to cover the testing of patches, which are submitted monthly by vendors, in order to integrate it in the NATO Environment.

Scope will include:

- Patches applied to current baseline in A2SL of Windows client and server operating systems and their compatibility with the existing NATO environment under NATO security settings and established security mechanisms.
- Patches applied to current baseline in A2SL of Linux client and server operating systems and their compatibility with the existing NATO environment under NATO security settings and established security mechanisms.

- **TST001-3 Commercial off the Shelf (COTS) Application Testing - Small:**

This package will consist of the effort required to test a new version of an already approved COTS application in order to integrate it in the NATO Environment. Small COTS applications are simple applications without any interoperability with other COTS or NOTS systems.

Scope will include:

- Installability and configuration of the COTS
- Compatibility testing with the existing NATO environment
- Correct functioning of the software under NATO security settings
- Correct functioning of the software under NATO security mechanisms.
- Compatibility testing with basic set of applications that will be utilized in the operating system

- **TST001-4 Commercial off the Shelf (COTS) Application Testing - Large:**

This package will consist of the effort required to test a new version of an already approved COTS application in order to integrate it in the NATO Environment. Large COTS applications are complex as they contain interoperability with COTS or NOTS systems or are complex in scope due to the functionality they provide.

Scope will include:

- Installability and configuration of the COTS
- Compatibility testing with the existing NATO environment
- Correct functioning of the software under NATO security settings
- Correct functioning of the software under NATO security mechanisms.
- Compatibility testing with basic set of applications that will be utilized in the operating system
- Limited interoperability testing required based on scenarios as deployed in NATO UNCLASSIFIED or NATO SECRET.

- **TST001-5 NATO off the Shelf (NOTS) Testing - Small:**

This package will consist of the effort required to test a new version of an already approved NOTS application in order to integrate it in the NATO Environment.

Scope will include:

- Installability and configuration of the NOTS
- Compatibility testing with the existing NATO environment
- Correct functioning of the software under NATO security settings
- Correct functioning of the software under NATO security mechanisms.
- No interoperability testing required

- **TST001-6 NATO off the Shelf (NOTS) Testing - Medium:**

This package will consist on effort required to test a new version of a NOTS system in order to be integrated in the NATO Environment. Medium NOTS applications have a limited number of interfaces with other COTS or NOTS.

Scope will include:

- Installability and configuration of the NOTS
- Compatibility testing with the existing NATO environment
- Correct functioning of the software under NATO security settings
- Correct functioning of the software under NATO security mechanisms.
- Limited interoperability testing required based on scenarios as deployed in NATO UNCLASSIFIED or NATO SECRET.

- **TST001-7 NATO off the Shelf (NOTS) Testing - Large:**

This package will consist on effort required to test a new version of a NOTS system in order to be integrated in the NATO Environment. Large NOTS are complex as they contain interoperability with COTS or NOTS systems or are complex in scope due to the functionality they provide.

Scope will include:

- Installability and configuration of the NOTS
- Compatibility testing with the existing NATO environment
- Correct functioning of the software under NATO security settings
- Correct functioning of the software under NATO security mechanisms.
- Expanded interoperability testing required based on scenarios as deployed in NATO UNCLASSIFIED or NATO SECRET.
- Compatibility with cross-domain services if required.

Service Request:

- The service request should include the amount per service flavour required. For example, for ACO the amount of evaluations of each type are based on the previous two years and it will be adapted for next cycle, as in the following table

number of units	Service Flavours	Remarks
2	TST001-1	Operating system testing
48	TST001-2	Patch Testing
220	TST001-3	COTS Testing – Small
110	TST001-4	COTS Testing – Large
72	TST001-5	NOTS Testing – Small
36	TST001-6	NOTS Testing – Medium
24	TST001-7	NOTS Testing – Large

- **Other:**
 - Additionally, nations may use the A2SL to inform their CIS Baseline or have other national processes to perform configuration change control on their CIS Baseline. Both may require testing services to fulfil their compliance to AC/322-D/0048-REV3.
 - Request made through a CRF if the customer is external or by providing OLA from an existing project.

Available on:

NATO Unclassified
NATO Secret

Service Prerequisites:

None

Underlying Services:

PLT008 – CTO NATO Software Factory

Standard Service support levels:

Testing Type	Average time to complete
Operating System Testing	4 weeks
Patch Testing	2 weeks
	1 week
COTS Application Testing – Small	1 week
COTS Application Testing – Large	4 weeks
NOTS Testing – Small	1 week
NOTS Testing – Medium	2 weeks
NOTS Testing – Large	4 weeks

In cases where there is missing required documentation, test licenses or SME support, the duration of testing cannot be predicted.

This service does not include the effort needed for service management and control processing nor cyber security assessment.

Service Reporting:

Every quarter (with the QSLR report) provide status updates on the following KPIs:

- Number and types of CRQs processed in the quarter
- Number of completed CRQs in the quarter
- Number of CRQs already in the backlog for next quarter
- New CRQs in the reporting quarter
- Quick summary of the highest visibility CRQs

Service Cost / Price:

The price is per flavour.

TST002 Interoperability Testing Service

Service ID: TST002

Service Name: Interoperability Testing Service

Portfolio Group: Testing Services

Service Description: This Service provides IT technical Interoperability testing. The service is used to test IT components, systems and integrated services with respect to their interoperability interfaces. The service contains a composition of integrated processes, skilled manpower and supporting toolset(s) to support IT technical interoperability testing during all stages of development and deployment of the components, systems or integrated capabilities in a variety of environments.

Value proposition:

The service combines planning, execution, reporting and assessment of interoperability testing. Some examples of this are:

- Federated Mission Networking Spiral specification testing;
- Interoperability testing at events of a variety of sizes;
- Support for operational interoperability testing based on actual mission CIS designs.

The customers the service delivers to are the NATO Command Structure, Project managers, Service Management Authorities of mission networks and individual nations that host/organize interoperability events.

Service Features:

The service always features the following components but the activities for each feature may vary depending on the service flavour :

- Test planning & Control
 - Reviewing the software requirements document (If any) and other related documents
 - Interviewing stakeholders to gather additional information, identifying (national) objectives
 - Identifying any ambiguities or inconsistencies in the requirements/ objectives
 - Identifying any missing or incomplete requirements/ objectives
 - Identifying any potential risks or issues that may impact the testing process and agree on level of risk to be accepted
 - Identifying windows of opportunity to group nations/ objectives into potential test opportunities
 - Updating CIS service designs
 - Output:
 - Forward schedule of Change
 - Detailed test schedule program for the next Quarter
 - Identified CIS service design changes to be tested (high level test plan)
- Analysis & Test design
 - Identifying the testing objectives and scope

- Developing a test strategy: selecting the testing methods and techniques that will be used
- Identifying the test cases that will be executed and the test data that will be used
- Estimating the time and cost required for testing
- Identifying the test deliverables and milestones
- Assigning roles and responsibilities to the testing team
- Reviewing and approving the test plan
- Output:
 - Test plan(s) with clear test scope, objectives and deliverables
- Test environment set up
 - Identifying the testing environment and resources needed
 - The necessary hardware, software, and network configurations set up for test execution
 - Installation and configuration of the necessary test support tools
 - Preparation of the necessary test data to support the execution
 - Output:
 - Prepared test environment for the execution of the plan (s)
- Evaluation & reporting
 - The test cases and scripts are run, and the results are collected and analysed
 - The results of the test execution are analysed to determine the software's performance and identify any defects or issues
 - Any defects that are identified during test execution are retested to ensure that they have been fixed correctly.
 - Test results are documented and reported to the relevant stakeholders
 - Plan and execute (daily) test meetings to understand issues, problems and adapt any plans if necessary
 - Output:
 - Test report(s)
- Test closure
 - The test environment is cleaned up, and all test data and test artefacts are archived.
 - Feedback from the testing process is collected and used to improve future testing processes (update SOPs, SOIs)
 - Knowledge about the software and testing process is shared with the rest of the team and any stakeholders who may need to maintain or support the software in the future.
 - Output:
 - Updated processes (SOP/SOI),
 - shared lessons identified,
 - clean test environment

Service Flavours:

- **TST002.1A - Small Event:** A small event is defined by the following parameters:
 - Up to 1 testing scenario

- Up to 10 participants
- Up to 10 services
- Up to 2 security domains

The following activities are costed:

- Lead and participate in planning conferences (1 conferences of 3 days)
- Lead and participate in test management workshops (1 workshops of 3 days)
- Plan, direct execution and report of Service V&V
- Plan, direct execution and report of Federation Joining V&V (2 days)
- Plan, direct execution and report of Federation V&V (3 days)

Deliverables:

- High Level test plan
- Detailed Test Plans with clear test scope, objectives and deliverables
- Detailed Test Reports
- Training package to participants on the process, the content and the toolset during the planning cycle and execution.
-
- **TST002.1B - Small Event with CFBLNet Lab Infrastructure:** A small event is defined by the following parameters:
 - Up to 1 testing scenario
 - Up to 10 participants
 - Up to 10 services
 - Up to 2 security domains

The following activities are costed:

- Lead and participate in planning conferences (1 conferences of 3 days)
- Lead and participate in test management workshops (1 workshops of 3 days)
- Plan, direct execution and report of Service V&V
- Plan, direct execution and report of Federation Joining V&V (2 days)
- Plan, direct execution and report of Federation V&V (3 days)
- Provision of lab infrastructure in support of the execution of the event connected to CFBLNet

Deliverables:

- High Level test plan
- Detailed Test Plans with clear test scope, objectives and deliverables
- Detailed Test Reports
- Training package to participants on the process, the content and the toolset during the planning cycle and execution.
- **TST002.2A - Medium event:** A medium event is defined by the following parameters:
 - Up to 1 testing scenario
 - Up to 15 participants
 - Up to 35 services
 - Up to 2 security domains

The following activities are costed:

- Lead and participate in planning conferences (2 conferences of 4 days / year)
- Lead and participate in test management workshops (1 workshops of 4 days / year)
- Plan, direct execution and report of Service V&V
- Plan, direct execution and report of Federation Joining V&V (1 week / year)
- Plan, direct execution and report of Federation V&V (1 week / year)

Deliverables:

- High Level test plan
- Detailed Test Plans with clear test scope, objectives and deliverables
- Detailed Test Reports
- Training package to participants on the process, the content and the toolset during the planning cycle and execution.
- **TST002.2B - Medium event with CFBLNet lab infrastructure:** A medium event is defined by the following parameters:
 - Up to 1 testing scenario
 - Up to 15 participants
 - Up to 35 services
 - Up to 2 security domains

The following activities are costed:

- Lead and participate in planning conferences (2 conferences of 4 days / year)
- Lead and participate in test management workshops (1 workshops of 4 days / year)
- Plan, direct execution and report of Service V&V
- Plan, direct execution and report of Federation Joining V&V (1 week / year)
- Plan, direct execution and report of Federation V&V (1 week / year)
- Provision of lab infrastructure in support of the execution of the event connected to CFBLNet

Deliverables:

- High Level test plan
- Detailed Test Plans with clear test scope, objectives and deliverables
- Detailed Test Reports
- Training package to participants on the process, the content and the toolset during the planning cycle and execution.
- **TST002.3A - Large event:** A large event is defined by the following parameters:
 - Up to 3 testing scenarios
 - Up to 50 participants
 - Up to 35 services
 - Up to 3 security domains

The following activities are costed:

- Lead and participate in planning conferences (4 conferences of 5 days / year)

- Lead and participate in test management workshops (2 workshops of 4 days / year)
- Plan, direct execution and report of Service V&V
- Plan, direct execution and report of Federation Joining V&V (2 weeks / year)
- Plan, direct execution and report of Federation V&V (3 weeks / year)

Deliverables:

- High Level test plan
- Detailed Test Plans with clear test scope, objectives and deliverables
- Detailed Test Reports
- Training package to participants on the process, the content and the toolset during the planning cycle and execution.

- **TST002.3B - Large event with CFBLNet Lab Infrastructure:** A large event is defined by the following parameters:

- Up to 3 testing scenarios
- Up to 50 participants
- Up to 35 services
- Up to 3 security domains

The following activities are costed:

- Lead and participate in planning conferences (4 conferences of 5 days / year)
- Lead and participate in test management workshops (2 workshops of 4 days / year)
- Plan, direct execution and report of Service V&V
- Plan, direct execution and report of Federation Joining V&V (2 weeks / year)
- Plan, direct execution and report of Federation V&V (3 weeks / year)
- Provision of lab infrastructure in support of the execution of the event connected to CFBLNet

Deliverables:

- High Level test plan
- Detailed Test Plans with clear test scope, objectives and deliverables
- Detailed Test Reports
- Training package to participants on the process, the content and the toolset during the planning cycle and execution.

Service Request:

- Through a CRF if the customer is external or by providing billable funds from an existing project.
- For example:
 - Request for FMN Framework CIAV:

number of units	Service Flavours	Remarks
1	APP117.2A	IO Toolset for Repository
2	APP117.2B	IO Toolset for Kanban
1	APP117.3A	IO Toolset in CFBLnet Pink
12	APP117.5B	Training Package for FMN CIAV
4	APP117.5C	
12	APP117.5D	
12	APP117.5E	
12	APP117.5F	
9	APP117.6	Premium support for FMN CIAV

- Request for NCSaaA CIAV:

number of units	Service Flavours	Test type
13	TST002.1B	Small Event with CFBLNet Lab Infrastructure (RFCs, Joining Event, Risk Reduction)
2	TST002.2B	Medium Event with CFBLNet Lab Infrastructure (eg: CJC2A, Risk Reduction Large)

- Request for VeVA Coalition Assurance and Validation: The amount of events of each type are based on the battlerythm setup by SHAPE.

number of units	Service Flavours	Test type
7	TST002.1A	Small Event (3xChange Management, 4xS&V for exercises)
3	TST002.2A	Medium Event (3xChange Management)
2	TST002.3A	Large Event (1xSTCO-A, 1XSTCO-B)
1	APP117.2 APP117.3 APP117.T (Packaged) APP117.P	IO Toolset Application Service
*NOTE: Testing for VeVA is performed in the VeVA MN and other corresponding networks used by the VeVA Initiative		



Available on:

Any network

Service Prerequisites:

APP117 – IO Toolset Service

Underlying Services: Interoperability Toolset Service

Standard Service support levels:

Testing Type	Average time to complete
Small event	2 weeks after execution
Medium event	4 weeks after execution
Large event	10 weeks after execution

Service Reporting:

Every Quarter (with the QSLR) report for the initiative flavour following the deliverables according to the yearly battle Rhythm

Service Cost / Price:

The unit of measure for all the flavours is per event. The price details for each of the service flavours is specified in the Costed Customer Service Catalogue (CCSC).



Application Services

This page is left blank intentionally

APP001 Approved Commercial-off-the-shelf Products Procurement Service

Please note that this service offering is for the provisioning of Commercial-off-the-shelf (COTS) software licenses and software support renewals. The products requested must be in the pool of the NCI Agency Approved Fielded Products List* (AFPL).

The costs for these products under this service are solely for the license procurement and/or annual software support renewal costs of the software license requested. It does not include any manpower support to package/install/maintain the application.

*If the product is not in AFPL, customers can choose to submit a separate CRF (Customer Request Form) in order to request the addition of this application to AFPL. The Agency applies a series of AFPL testing procedures before it can confirm that the application can be added to AFPL or not, thus separate costs apply to such requests and are not considered within the scope of APP001.

APP001A Supported Commercial-of-the-shelf (COTS) Business Applications

Service ID: APP001A

Service Name: Supported Commercial-of-the-shelf (COTS) Business Applications

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Available

Service Description: Please note that this service offering is for the provisioning of Commercial-off-the-shelf (COTS) Business Applications. The products requested must be in the COTS Business Applications Catalogue¹.

If the product is not in COTS Business Application Catalogue, customers can choose to submit a separate CRF (Customer Request Form) in order to request the addition of this application to A2SL and to the COTS Business Application Catalogue. The Agency applies a series of A2SL testing procedures before it can confirm that the application can be added to A2SL or not, thus separate costs apply to such requests and are not considered within the scope of APP001A.

The costs for these products under this service are solely for the license procurement and/or annual software support renewal costs of the software license requested as well as limited manpower support to package/install/maintain/patch the application on the NCIA Managed Networks.

Value Proposition:

Centralize the request and provisioning of Applications ensuring compliance with NATO and Agency processes as well as maintain an updated A2SL list.

Service Features:

Service features are grouped into service flavours as below:

Free COTS

Client applications that are deployed on end user devices (workstation) of simple complexity or cloud applications with access granted per user.

Example: KeePass, 7ZIP

Simple COTS

¹ If the product is not in COTS Business Application Catalogue, customers can choose to submit a separate CRF (Customer Request Form) in order to request the addition of this application to A2SL and to the COTS Business Application Catalogue. The Agency applies a series of A2SL testing procedures before it can confirm that the application can be added to A2SL or not, thus separate costs apply to such requests and are not considered within the scope of APP001A

Client applications that are deployed on end user devices (workstation) of simple complexity or cloud applications with access granted per user.

Example: Adobe, Autodesk Products

Medium COTS

Web application requiring maximum one web server and a database.

Example: TeamMate+

- **Activities in scope of this Service:**

Service Management of entire service lifecycle including regular user communication;

Supplier Management:

- Management of the required 3rd party contracts (contract signature, extension or termination as required)
- Monitor delivery of 3rd party services/goods;

Application Management:

- **Independent Verification & Validation:**
 - Change Configuration Proposal (CCP) Submission and Follow up;
- **Incident Management:**
 - Issue Investigation and Resolution; Escalation of tickets to 3rd party supplier when required and follow up until their final resolution;
- **Deployment:**
 - Configuration & Reconfiguration;
 - Deploying & Release, and Patches Management;
- **Maintenance and Support:**
 - Operate and perform the required maintenance on the application servers and the underlying platform.
 - Operate and perform the required maintenance on the databases including backup, restore and replication.
 - KPI Monitoring as per reporting features
 - Maintenance of the related AD Components;
 - Set up and Maintenance required Reference/Test and Development environment in NSF

Service Request:

1. Request of COTS in the COTS Business Application Catalogue and A2SL:

Service Request and/or CRQ on ITSM only to install COTS. Reconciliation between number of available and installed licenses are part of QSLR process.

2. Request of COTS not included in to COTS Business Application Catalogue

CRF process and additional costs.

Available on: NU, NS, NR, MS, NPCL and other CIS

Service Prerequisites (only for NCIA managed networks):

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side).
WPS002 User Access Services
WPS008 Operations Centre Service
SEC015 Security Certificate Service
LEG008 Local Other Service

Service Cost / Price:

The cost is calculated per user licence allocated/deployed, the licence cost is not included in the service cost.

The price details available in the Service Rates document and in the COTS Business Applications Catalogue.

Service ID	Description	Unit of Measure	Comments
APP001A – 1	Free COTS	Per user	Minimum quantity 1000
APP001A – 2	Simple COTS	Per user	Minimum quantity 100
APP001A – 3	Medium COTS	Per user	Minimum quantity 10

APP002 Shared Early Warning (SEW) Application Service

Service ID: APP002

Service Name: Shared Early Warning App

Portfolio Group: Application Services

Service Description:

NATO Shared Early Warning (SEW) is NATO's early warning capability to disseminate Theatre Ballistic Missile (TBM) launch data to higher military command levels and political representatives in NATO and NATO Nations. SEW forwards BM launch warnings provided by the USA about ballistic missile launches that occur within an agreed distance around NATO territory, regardless of the predicted impact area.

SEW increases the situational awareness of the NATO decision makers involved in Ballistic Missile Defence (BMD) and supports the process of taking accurate and timely measures to counter BM strikes or any other countermeasure to limit/avoid damage to Allies. Additionally national civil defence agencies need early warning of attacks in order to support passive defence measures for their populations.

A Ballistic Missile (BM) is defined as any missile that does not rely upon aerodynamic surfaces to produce lift and consequently follows a ballistic trajectory when thrust is terminated. Short Range Ballistic Missiles (SRBMs), Medium Range Ballistic Missiles (MRBMs) and Intermediate Range Ballistic Missiles (IRBMs) are reported through NATO-SEW. Intercontinental Ballistic Missiles (ICBMs) and Space-Launch Vehicles (SLVs) are currently under testing and they are planned to be reported in the future. The reporting area is described as the "NATO-SEW Threat Region". Voice early warning and/or warning confirmation will typically follow data warning. United States European Command (USEUCOM) acts as the chief USA liaison to NATO concerning NATO-SEW operations [ACO Directive 80-66].

Value proposition:

The scope of the system is twofold:

- The main purpose of the early warning information in peacetime is to update NATO HQs and nations about ongoing BM launches in order to complement their overall intelligence assessment.
- During crisis and conflict, the early warning information will become an important factor in the overall intelligence assessment. It will be used to inform military units and populations in the crisis area of the general likelihood of BM attacks and of the details of BMs possessed by a potential adversary. This information will be used for operational considerations, e.g., deployment of TMD units, readiness postures, etc. Designated active TMD units in the crisis area will be alerted to prepare their systems for ActD and to expect an inbound BM on a predicted trajectory for engagement.

Service Features:

- **Service Delivery Point (SDP) activation** provides technical advice to the local CIS engineers who install SEW through the NCIA DML (under licence agreement) and connection to the SEW data stream

- **SDP Remote Support** provides centralised assistance and advice to local Support Engineers who maintain the SEW SDP.
- **SDP Management** includes “SDP Remote Support” and complements with a local footprint for technical support. Remote administrator access required.
- **Service Access Point (SAP) activation** provides configuration of on-site user access to an existing SEW SDP.
- **SAP Remote Support** provides centralised assistance and advice to resolve incidents and/or address service requests via NATO/NCIA ITSM ticketing system to log, categorize and escalate if applicable. By default, includes 12 tickets per SAP. No remote power-user access is required.

Service Flavours: The service is available with the following flavours:

APP002-1 SEW Product Lifecycle: This service flavour provides centralized application maintenance and availability of the SEW service for the Bi-SC and for ACO exercises planning cycle for the current year.

APP002-2 SEW for an Organisational Entity (NCS-A) or NATO Mission: This service flavour provides full SEW usage for an Organisational Entity (NCS) or NATO mission. It includes three instances in the Service Delivery Point; operational, exercise and training. The support is planned up to 200 users. It includes remote and on-site mentoring.

APP002-3 SEW for a Federated Entity: This service flavour provides federation support to NFS and Nations for authorization, configuration and troubleshooting of their connections to a SEW Service Delivery Point (identified as centralized NCS Col servers).

This flavour also encompasses Application changes triggered by federation requests and compensation for capacity increase required by the increasing demand on corresponding centralized infrastructure.

Types of possible federations are:

B2C: remote connection to centralized SDP (up to 20 users)

B2B: synchronisation connection to centralized SDP

E2E: managed sessions to centralized SDP (up to 20 sessions)

This service flavour ensures initialization and continuity of the COI interconnections between Nations & NFS with NCS. Troubleshooting beyond NATO Interconnection Point on the national or NFS side is not included in this service flavour. The service flavour offers:

- Management of technical connectivity to centralized NCS COI servers given the requester has authorization from SHAPE and the corresponding NCS party
- Troubleshooting on configuration of the connection to centralized NCS COI servers
- Application service delivery monitoring & corrective actions

- Application changes triggered by this federation request
- Compensation for capacity increase as per the increasing demand on corresponding NCS Col servers

ICT support services to External Customers is recommended to complement this flavour, would the Customer have connectivity in B2B mode. This is recommended for support beyond NIP.

APP002-4 SEW in a NATO Exercise: This service flavour provides standard exercise planning and execution support for NATO exercises. It includes exercise design review, dedicated exercise configuration, and after-action analysis report for any NATO exercise. Planning excluded (already included in Product Lifecycle flavour).

Available on:

All NATO and National networks

APP002-3 SEW for a Federated Entity: NATO Secret

Service prerequisites: Infrastructure compatible with the requirements of the SEW application as described in the Release documentation.

APP022-FED: Network connectivity for NIP interconnection with NATO centralized network (NS).

Underlying Services: PLT008, OTH001, SME005

Standard Service support levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Available NCI Academy Training not covered by service cost: Not applicable for SEW

Service Cost / Price: The unit of measure for the Service is 1 for APP021-1 flavour.

For APP002-2, the unit of measure is the site utilizing the service (per site).

For APP002-3, the unit of measure for the Service is per connection.

For APP002-4, the unit of measure is the exercise where the service is used (per event).

The price details for each of the service flavours is specified in the Costed Customer Service Catalogue (CCSC).

APP005 CBRN Application Service

Service ID: APP005

Service Name: CBRN Application Services

Service Type: Customer Facing

Portfolio Group: Application Service

Service Description

The Chemical, Biological, Radiological, and Nuclear (CBRN) Application Services provides functions that enable CBRN Community of Interest to support the three pillars of CBRN Defence – Prevent, Protect and Recover.

Value Proposition

The service is integral to the NATO CBRN Community of Interest and offers the following benefits:

- Maintenance of CBRN applications in accordance with the NATO specific requirements and the latest doctrine;
- Provision of state of the art service assets that support the CBRN community to:
 - Establish and maintain CBRN situational awareness in NATO missions and operations;
 - Calculate the NATO approved hazard areas and contaminated areas for all types of CBRN incidents;
 - Perform hazard estimation after TBM engagement;
 - Support risk assessment and what-if analysis of known or potential hazards within operational areas;
 - Generate of exercise planning material based on pre-planned incidents;
- Training and support in the usage of CBRN applications assets in support of NATO missions and operations.

Service Features

The main service consists in the provision of the following service features:

- Centralised acquisition and management of CBRN application licenses, export authorisations and vendor logistics support;
- Support of the applications accreditation process for NATO security domains;
- Support change and configuration management processes;
- Installation and configuration of software application instances;
- In-service support
 - Centralised routine support: the regular maintenance of the software applications on the NATO networks including:
 - Overall service management and planning;
 - Maintenance and communication of the service roadmap;
 - Support and maintain the accreditation of the CBRN application assets;

- Centralised support provided to the CBRN community of interest;
- Analysis of incidents and problems related to the operation of CBRN applications;
- Coordination of the investigation of issues and requirements with the respective software vendors;
- Management of service requests;
- Specific service instance support: provides the required individual support services to the specific sites at charge and may include:
 - Support to design, planning and implementation of the CBRN application services at the site;
 - Online support regarding incidents and service requests related to the installed CBRN application assets;
 - Implementation of the required software updates in accordance with the service roadmap;
- Training on the usage of CBRN applications aligned with the NATO doctrine and best practices.

The service includes the following application assets:

- **CBRN Analysis**
An advanced, COTS-based CBRN defence information management application that includes hazard prediction and warning and reporting (W&R). Provides users with rapid and accurate information to increase their CBRN situational awareness within an area where CBRN materials may be used. CBRN Analysis effectively supports and enhances risk-management in all phases of an operation, both in the planning and pre-deployment phase, in-theatre and in the post conflict or recovery phase. NATO currently uses 40 licenses, distributed over the various sites.
- **HPAC - Hazard Prediction and Assessment Capability**
HPAC models the release of CBRN materials to the atmosphere and the associated dispersion using detailed meteorological information.
Note: SHAPE governs the release of this application.
- **HEAT - Hazard Estimation After TBM Engagement**
HEAT offers capabilities to determine consequences of intercept and consequences of non-intercept estimations and reporting during BMD and CBRN Defence mission execution. HEAT is a German VNC desktop-only applications.

Service Flavours

APP005-1 CBRN Analysis Product Lifecycle Support – This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of CBRN Analysis regardless of the number of sites using the product. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year. The product lifecycle support unit of measure is unit 1.

APP005-2 CBRN Analysis Standard Instance – This flavour provides for a CBRN Analysis instance on specified network domain with its own specific setup, configuration and user access. This includes the prerequisite hosting infrastructure and platform of the instance on specified network domain, the maintenance and support for the infrastructure, platform and running instance, such as OS upgrades, application upgrades and hot-fixes, and backup and recovery management during one year.

APP005-3A CBRN Analysis Standard Support Small Site (1-10 Users) – This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 10 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.

APP005-3B CBRN Analysis Standard Support Medium Site (11-25 Users) – This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 25 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.

APP005-4 CBRN Analysis User License (Renewal and additional) – This flavour is for the renewal of existing and procurement of additional licenses of CBRN Analysis valid for one calendar year. This flavour does not include implementation and follow-on in-service support.

CBRN Analysis Standard Support Large Site (26> Users) (Custom Rate) – This custom flavour offers the same as flavour APP005-3B for sites/network domains with over 26 users.

APP005-5 HPAC Product Lifecycle Support – This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of HPAC regardless of the number of sites using the product. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year. The product lifecycle support unit of measure is unit 1.

APP005-6 HPAC Standard Instance – This flavour provides for a HPAC instance on specified network domain with its own specific setup, configuration and user access. This includes the prerequisite hosting infrastructure and platform of the instance on specified network domain, the maintenance and support for the infrastructure, platform and running instance, such as OS upgrades, application upgrades and hot-fixes, and backup and recovery management during one year.

APP005-7A HPAC Standard Support Small Site (1-10 Users) – This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 10 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.

APP005-7B HPAC Standard Support Medium Site (11-25 Users) – This flavour offers user access management and user support for all levels of users. The flavour applies to one site

for up to 25 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.

HPAC Standard Support Large Site (26> Users) (Custom Rate) – This custom flavour offers the same as flavour APP005-7B for sites/network domains with over 26 users.

APP005-8 HEAT Product Lifecycle Support – This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of HEAT regardless of the number of sites using the product. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year. The product lifecycle support unit of measure is unit 1.

APP005-9 HEAT Standard Instance – This flavour provides for a single running copy (instance) of HEAT on specified network domain with its own specific setup, configuration and user access. This includes the prerequisite hosting infrastructure and platform of the instance on specified network domain, the maintenance and support for the infrastructure, platform and running instance, such as OS upgrades, application upgrades and hot-fixes, and backup and recovery management during one year.

APP005-10A HEAT Standard Support Small Site (1-10 Users) – This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 10 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.

APP005-10B HEAT Standard Support Medium Site (11-25 Users) – This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 25 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.

HEAT Standard Support Large Site (26> Users) (Custom Rate) – This custom flavour offers the same as flavour APP005-12 for sites/network domains with over 26 users.

CBRN Applications Training (Custom Rate) – This custom flavour offers bespoke training for the CBRN Applications.

CBRN Applications On-Site Support (Custom Rate) – This custom flavour offers on-site functional and/or technical support.

CBRN Applications Exercise Support (Custom Rate) – This custom flavour offers functional and/or technical support during an exercise above and beyond the support already covered within CSLA.

CBRN Applications New Site Implementation Support (Custom Rate) – This custom flavour is for the deployment and early-life support for one or more CBRN applications at a site/network domain.

Available On

- NATO Secret;
- Mission Secret;
- VeVA;
- Deployable CIS.

The application service may be made available on other security domain/networks which will be assessed upon a new customer service request.

Service Prerequisites

- NDW002 NATO Digital Workplace Service (High Side) - for application instances installed on NCI Agency managed networks;
- WPS004 - Email Service;
- APP055 - Core GIS: for Open Geospatial Consortium (OGC) compliant map services.

Standard Service Support Levels

- **Service Availability Target:** 95.0%
- **Service Restoration:** This service is included as critical service, the service restoration period for widespread outage within NCS is 8 hours Wall Clock (P2+), otherwise a lower priority will be assigned.

N.B.1: Availability and restoration times of the CBRN applications services are primarily dictated by the availability of the underlying services.

N.B.2: Full priority resolution times and generic service priority assignment matrix will be adhered to in accordance with the defined service level agreement.

Service Reporting: Periodic reporting as agreed with the customer.

Training:

No NCI Academy training courses are available nor is any training covered within the service rate; Training can be provided upon a new customer service request.

Service Cost / Price:

The cost of the service is composed of a product life cycle support cost, which is a necessary cost to keep the product running regardless of the number of sites running the application; the product lifecycle support flavour unit of measure is 1. There is also a cost for deployment and support flavours depending on the size of the site. The unit of measure for these flavours is per instance and per site respectively. The cost details are listed in the service rate section of this catalogue release, except for the “custom” flavours. For the “custom” flavours, the unit of measure is 1 at a custom rate.

APP006 Ballistic Missile Defence (BMD) System of Systems Management Service

Service ID: APP006

Service Name: Ballistic Missile Defence (BMD) System of Systems Management

Portfolio Group: Application Services

Service Description: The APP006 service provides coordination and orchestration of In Service Support activities related to BMD System of Systems including interoperability assurance, integration and lifecycle management, and provides the Shared Early Warning Plus service (SEW+I). The service also provides the primary interface between the customers and users (Operational BMD Community) and all NCI Agency Units devoted to perform In-Service Support (ISS) for the BMD Command Control Communication and Information (BMDC3I) System of Systems. The service does not take over or duplicate any of the below defined BMDC3I services.

The BMD capability: Provides full coverage and protection for all NATO European populations, territory and forces against the increasing threats posed by ballistic missiles. This also includes required protection of deployed forces and high value assets/areas within an area of operations/interest from attacks by ballistic missiles. BMD interlinks all levels of military command from the military strategic level down to the tactical level, all across NATO, regardless of the country or the respective military service. BMD is a combined and joint capability.

BMD System of Systems: The NCI Agency IT Systems (products and services), in support of the BMD capability, provide functions that enable NATO Commands to integrate sensor information, build and distribute a comprehensive and real-time BMD operational picture, and exercise command and control of voluntary national contributions (sensors and effectors) provided by Allies. The application Air Command and Control System TMD1 (APP050) is the core integrator of the BMD functions.

The BMDC3I systems are in use at the Ballistic Missile Defence Operations Centre (BMDOC) in Ramstein and multiple other NATO Command Structure sites. The following products and services enable the BMD capability and compose the BMDC3I System of Systems:

Customer facing services:

- APP002 (SEW Application Service) Shared Early Warning
- APP007 (TOPFAS Application Service) - Tool for Operations Planning Functional Services
- APP015 (JCHAT Application Service) - Secure Tactical Joint Chat
- APP022 (NCOP Application Service) - NATO Common Operational Picture
- APP049 (ICC Application Service) - Integrated Command and Control (includes LSID)
- APP050 (Air Command and Control System TMD1)
- APP061 (AirC2IS Application Service) - Air Command and Control Information System

- WPS014 (Secure Voice Service)
- WPS015 (Voice Loop Service)

Other supporting services:

- APP010 (NIRIS Application Service) - Networked Interoperable Real-Time Information Service
- APP011 (OANT Application Service) - Online Analyser for Networked Tactical-Data
- APP012 (SMACQ Application Service) - Service to Monitor and Assess Connectivity and Quality
- PLT013 (NISP Service) NATO - Integrated Secure Platform
- APP055 (Core Geographic Information System -GIS- Application Service)
- WPS002 (Enterprise Identity Access Management Service)
- WPS003 (Enterprise User License Service)
- PLT001 (Information Sharing and Collaboration Platform Services)
- WPS012 (E-mail Service)
- PLT003 (Web Hosting Service)
- SEC011 (Gateway Security Service)
- INF001 (LAN Service)
- INF002 (NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service)
- INF004 (Infrastructure Virtualization Service)
- INF005 (Infrastructure Integration Service)
- INF006 (NATO Enterprise Directory Service -NEDS)
- INF007 (Infrastructure Storage Service)
- INF014 (Transmission Service)
- INF018 (Deployable CIS Mini-Point of Presence (PoP))
- INF040 (UHF TACSAT Radio Services) - Tactical Satellite

The actual BMDC3I service composition for operational use depends on the customer's operational requirements. NCI Agency configures the required composition in close cooperation with the customer.

All above listed BMDC3I services operate on the NATO General Communications System (NGCS) network at Wide Area Network level. Nations provide feeds through NATO-National static gateways or through NATO deployable CIS equipment.

Value proposition: The Service main objective and value is to maintain the availability, integrity and alignment of the fielded BMD Command Control Communication and Information (BMDC3I) System of Systems and the IT services provided by NCI Agency for BMDC3I. The service also provides coordination of actions for BMD In-Service Support related aspects and issues for NATO BMDC3I customers and users.

Service Features: The APP006 service manages the following in support of BMDC3I system of systems:

- the BMD SoS Delivery Plan in accordance with the BMD SoS Service Tree.

- The supervision of the processing of ISS ITSM BMD related Tickets (Incident, Services Requests) through their lifecycle and monitoring iaw SLA levels.
- the processing of ISS BMD related L-ECPs, and monitoring of their implementation plan/execution.

the relationship with CSU Ramstein and BMDOC users: Ensure day-to-day coordination with them related to BMD Standing Mission, NS2T Mission, technical evaluation activities, Site Support Manager Role and CAB chairmanship.

- BMD Obsolescence Management: Manage BMD SoS obsolescence; maintaining risk review and gap analysis of the SoS and interconnecting systems in coordination with other Service Lines and system owners. This analysis will consider programmatic and funding mechanisms to ensure the SoS components and services are supported throughout the lifecycle.

Service Flavours: The service is available as a single flavour

Available on: N/A

Service prerequisites: None

Standard Service Support Levels: N/A. The APP006 service supports at coordination level all NCIA Service Lines to provide In-Service Support in accordance with requirements as agreed between the Customer and NCI Agency for BMDC3I related services).

Available NCI Academy Training not covered by service cost:

A1027	APP006	BMD Planning with AirC2IS

Service Cost / Price: The unit of measure for the Service is 1. NCI Agency charges the total of the Service delivery in accordance with specifically arranged conditions of the Service delivery. The service APP006 does not duplicate any of the service delivery costs for the above-mentioned BMDC3I System of Systems services.

APP007 TOPFAS Application Service

Service ID: APP007

Service Name: Tools for Operations Planning Functional Services (TOPFAS) Application Service

Service Type: Customer Facing

Portfolio Group: Application Services

Service Status: Available

Service Description: TOPFAS (Tools for Operations Planning Functional Services) Application Service provides the user with integrated collaboration planning and decision support capabilities. This service is comprised of multiple modules that support Systems Analysis, Operational Planning, Order of Battle (ORBAT) management and Assessment of Operational Campaigns. This service also offers complete support for the NATO Force Generation Management process and Readiness Reporting as well as non-Intel Request For Information (RFI) Management.

Value Proposition: TOPFAS Application Service offers the user (through the suite of available modules) a distributed, multi-level and a collaborative environment that benefits standardization, productivity and quality to operational planning processes. TOPFAS offers a unique combination of desktop applications, web applications and portal to provide dedicated tools and information dissemination to each community of interest. Furthermore, the TOPFAS Application Service also contributes to the Ballistic Missile Defence capability through integration of specific functions and interfaces for BMD, in particular with AirC2IS.

Service Features: The TOPFAS Application Service is comprised of the following applications:

- TOPFAS Systems Analysis Tool (SAT) – Supports systems analysis of the engagement space for holistic situational awareness and understanding.
- TOPFAS Operations Planning Tool (OPT) – Campaign planning tool that supports the development and synchronization of strategic options, operational and tactical courses of action
- TOPFAS Campaign Assessment Tool (CAT) – Supports measuring progress towards the planned campaign end-state.
- TOPFAS ORBAT Management Tool (OMT) – Supports building and viewing order of battle (ORBAT) information and allows for management of national and NATO Response Force (NNRF) ORBATs.
- TOPFAS Web Portal and Applications (TWP) – Provides TOPFAS information content to be shared with wider communities of interest through an internet portal as well as dedicated applications for Wiki, RFI, Videos, etc.
- TOPFAS NATO Response System (NRS) Applications – Web based tool – Supports the formal declaration and approval processes of Responses Measures by SHAPE and Nations.
- TOPFAS enhanced Force Generation Management Tool (eFGMT) – Web based tool – Supports the complete NATO Force Generation cycle with nations

- TOPFAS Readiness Reporting Tool (RRT) – Web based tool – Supports the evaluation readiness of the NATO Response Forces or coalition forces
- TOPFAS Operational Capability Concept (OCC) Evaluation and Feedback (E&F) Tool – Supports partner efforts to develop forces that are fully interoperable and capable of operating with NATO

In addition, these services include the delivery and maintenance of support applications and portals:

- TOPFAS User Management Tool (UMT) – Allows TOPFAS functional managers to manage user access and roles
- TOPFAS Data Management Tool (DMT) – Allows TOPFAS reference data and configuration management
- TOPFAS Support Portal – Information SharePoint portal;
- TOPFAS Help Centre - Online help, Computer Based Training and support portal.

Service Flavours: The unit of measure for the Service is an HQ (small or large). The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Service Name	Service Flavour / Option	Service Unit	Package
TOPFAS Application Service	APP007-1 Product life cycle	1	Product lifecycle support
	APP007-2 TOPFAS Instance Support	Instance	Support
	APP007-3 User Support	Site	Support

APP007-1 Product lifecycle support – this flavour includes the activities to provide centralized baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management and service delivery management during one year.

APP007-2 TOPFAS Instance support - This flavours provides for a single running copy (instance) of an application on specified network domain with its own specific setup, configuration and user access. This includes the hosting infrastructure and platform of the instance on specified network domain, the maintenance and support for the infrastructure, platform and running instance, such as OS upgrades and application upgrades and hot-fixes, and backup and recovery management.

APP007-3 User support – This flavour offers user access management and user support for all levels of users. The flavour includes provision of centralized technical support, incident

management, request fulfilment, access management, and problem management during one year.

Available on: NATO Secret, Mission Secret

If you require availability of any other security domain please raise this as a New Service Request.

Service Prerequisites:

- NDW002 NATO Digital Workplace Service (High Side).
- APP055 - Core GIS Geospatial Services

Standard Service Support Levels:

Service Availability¹ Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting: Standardised service reporting to customers in accordance with the NCI Agency SLAs

Available NCI Academy Training not covered by service cost:

A0264	TOPFAS System Administrator
A0265	TOPFAS OPT for User
A0266	TOPFAS SAT for User
A0267	TOPFAS CAT for User
A0285	TOPFAS OPT Train the Trainer
A0286	TOPFAS SAT Train the Trainer
A0287	TOPFAS CAT Train the Trainer
A0288	TOPFAS for Advanced User
A9067	eFGMT Functional Manager
A9068	eFGMT Practitioner

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

Service Cost

The cost of the service is composed of a product life cycle support cost, which is a necessary cost to keep the product running regardless of the number of sites running the application; the product lifecycle support flavour unit of measure is 1. There is also a cost for deployment and support flavours depending on the size of the site, the unit of measure for these flavours is per instance and per site respectively. The cost details are listed in the service rate section of this catalogue release.

APP010 NIRIS Application Service

Service ID: APP010

Service Name: NIRIS Application Service

Portfolio Group: Application Services

Service Description: The NIRIS (Networked Interoperable Real-Time Information Service) Application Service provides situational information in support of automated (Air) C2 and information systems as well as BMD System of Systems within NATO. The NIRIS Application Service does this through the enablement of data collection, dissemination and transformation to information in an interoperable manner, based upon NATO and Commercial standards.

Value proposition: The NIRIS Application Service is integral for communities of interest within Air, Land, Maritime, Joint, Logistic and Intelligence domains. The NIRIS Application Service acts as a middle layer between data producers and information consumers (e.g. ICC, AirC2IS, NCOP and iGeoSIT) making information collected from multiple sources available to decision makers (as services) as Battle Space Objects (BSO). The key values of NIRIS are:

- Provision of (near) real-time situational awareness for operations.
- Wide range of supported interfaces for data collection and exchange strongly supporting interoperability.
- Harmonised view via BSO's on the collected data with access to in-depth detail to support decision makers.
- Allows integration via several standardised interfaces with other NATO and National systems.

Service Features: The NIRIS Application Service features the ability for data collection, dissemination and transformation of data in an interoperable manner based on NATO and commercial standards. Furthermore, it provides services to perform data format conversions, recording/replay and track augmentation. Management of NIRIS is offered by a modern, web-based user interface offering full, role-based access to the various capabilities. A key feature is the versatility of its interoperability while maintaining focus on standard's compliance. The main supported interfaces for data collection and exchange are:

- Link1 (STANAG 5501) – Air Picture
- Link 11B (STANAG 5511) – Maritime, Air Picture
- Link 16 (STANAG 5516) – Air, Ground, Maritime, BMD Picture
- JREAP (STANAG 5518) – Transport for Link 16
- VMF (MIL-STD-6017) – Ground Picture
- Link 22 (STANAG 5522) – Maritime, Air Picture
- OTH-T-Gold – Maritime, Ground, Air Picture
- Automatic Identification System (AIS) – Civilian Maritime Picture
- NFFI ("D" Doc) – Friendly Force Tracking (Ground) Picture
- FFI-MTF-XML (STANAG 5527) – Friendly Force Tracking (Ground) Picture
- SIMPLE (STANAG 5602) – Transport for Link 11, Link 16, Link 22, DIS (for IO testing)
- ITV and VATS – Civilian Convoys
- Eurocontrol ASTERIX (including ADSB) – Civilian Air Picture and Air Traffic Control

The collection and exchange is utilizing standard protocols where available (both IP and serial). The NIRIS Application Service offers full hub capabilities for e.g. Link16/JREAP, Link1, FFT and SIMPLE, including extensive filtering options.

The main supported interfaces for data and information consumers are:

- Trackstore integration (via Java API) – Provision of (near) real-time BSO information
- RESTful Track Service (JSON) – Provision of near real-time BSO information
- NVG (NATO Vector Graphics) – BSO overlays via web-services
- KML (Keyhole Mark-up Language) – BSO overlays via web-services
- SIP3 – Friendly Force Tracking information via web-service interface (NFFI, FFI)
- WSMP (Web Service Messaging Protocol)

Service Flavours: The service is available as the following flavours.

Service Name	Service Flavour / Option	Service Unit	Description
NIRIS	APP010-1 NIRIS Product LifeCycle Support	1	Product Lifecycle Support service includes the activities to provide centralized baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management and service delivery management during one year.
	APP010-2A NIRIS Deployment Small Site	1 Site	The product unit includes preparation, installation, configuration, verification, documentation and ELS for a small site with max. 5 sources and 1 type of consumer.
	APP010-2B NIRIS Deployment Medium Site	1 Site	The product unit includes preparation, installation, configuration, verification, documentation and ELS for a medium site with max. 10 sources and 2 types of consumers.
	APP010-2C NIRIS Deployment Large Site	1 Site	The product unit includes preparation, installation, configuration, verification, documentation and ELS for a large site with max. 15 sources and 3 types of consumers
	APP010-3A NIRIS User Support Small	1 Site	The product unit includes support for 1 calendar year for a small site.

	APP010-3B NIRIS User Support Medium	1 Site	The product unit includes support for 1 calendar year for a medium site.
	APP010-3C NIRIS User Support Large Site	1 Site	The product unit includes support for 1 calendar year for a large site.
	APP010-4 Feasibility Study	1 Study	The Study depicts the requirements of the customer, Information Exchange Requirements (IERs) and a proposed architecture
	APP010-5 Technical Workshop (on-site)	1 Site	The product unit includes an on-site workshop for 5 days (including travel)

Available on:

NATO Unclassified

NATO Secret

Mission Secret

Availability on any other security domain is TBC upon a New Service Request.

Service Dependencies:

SEC011: Security Certificate Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A1012	NIRIS Basic System Administrator
A1028	NIRIS Advanced System Administrator

Service Cost / Price:

The unit of measure and price details for each of the service flavours is specified in the Costed Customer Service Catalogue, except for the “custom” flavours. For the “custom” flavours, the unit of measure is 1 at a custom rate.

The total of the service delivery cost is charged in accordance with specifically agreed dimensions and conditions of each service delivery flavour, i.e. a defined flavour unit rate multiplied by the quantities (units) to be consumed.

APP011 OANT Application Service

Service ID: APP011

Service Name: OANT Application Service

Portfolio Group: Application Services

Service Description:

In data-driven organizations, success is based on high-quality data. Reliable insights and well-informed decisions stem from accurate and consistent data. By adopting strong data quality frameworks, prioritizes data integrity based on well-defined standards, NATO maximizes the value of their data assets, driving smarter and correct decisions, therefore gaining a competitive advantages.

The OANT (Online Analyser for Networked Tactical-Data) Application Service provides its users with a quick and easy way to analyse C4ISR data flowing on operational, test and/or exercise dissemination networks. It provides compliancy reports to agreed NATO Standards, plus providing Revision, Extract and Report capabilities on the connectivity of the data flows. Furthermore the provision of capability in the checking of data quality.

The OANT Application Service provides a web-based net-enabled service interface for data monitoring, analysis and reporting, supporting various operational data exchange formats and protocols (here called data flows) such as: JREAP, GMTI, Link 16, Link 11, Link 1, NFFI, FFI, DIS, OTH-G and more.

Value proposition:

The OANT Application Service provides its users with the following number of key benefits:

- NATO Standardization and Standards V&V bodies: test and verify quality and improve content of STANAGs for completeness, correctness, ambiguities and vagueness.
- War fighters (J3 and J6): up-to-date web access to shared assessments and improved situational awareness of data flows, connectivity and exchanged data quality, increasing trust in the information used to support decision making.
- OPS and interoperability event network, service management and control and analysis groups: smarter, improved and shared means of monitoring connectivity and data quality, to identify, understand and troubleshoot data and interoperability issues in a timely manner.
- System/Service developers: cost and time-savings with improved insight into STANAG compliancy and data content of exchanged messages to support self-analysis and continuous “pretesting” in order to foster out-of-the-box plug-and-play interoperability.

Service Features:

The OANT Application service is comprised of the following features:

- Enablement of one-to-one mapping between Standard Specifications and the way OANT interprets messages, words and fields;
- Interpretation of received messages from bits and bytes into human readable information;
- Assessments of received message contents against applicable standards leveraging on XML generated metadata and data specifications captured in-line with the STANAG/Standards Transformation Framework (STF) Design Rules (NISP, 2014);
- Collection and reporting of statistics on received data (including but not limited to breakdown per payload format, message originator, message label and encountered error type);
- Provision of further insight in to derived message information (e.g. track information);
- Interface for data monitoring, analysis and reporting, supporting various operational data exchange formats and protocols, such as JREAP, GMTI, Link 16, Link 11, Link 1, Link 22, VMF, SIMPLE, NFFI, FFI, DIS and OTH-G;
- Provision of analysis and verification of a data forwarding process; comparing both the input the stream and the forwarded data stream; and providing an assessment of whether the forwarding occurred in accordance with the applicable data forwarding standard.

SMACQ (APP012) and OANT (APP011) together form the C2 IOTA (Command and control data interoperability and traffic assessment) Services Suite.

Service Flavours:

APP011-1 OANT product Lifecycle Support: This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of the specified application. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year.

APP011-2A – OANT Small Instance:

This flavour provides the required support in deploying (or updating) the OANT Application Service and it consists of:

- a) Deployment of (up to) 1 instance of OANT with (up to) 5 data streams analysers (basic, bidirectional or proxy) based on the protocols supported by the OANT software (see OANT Application Service documentation);
- b) Configuration of the (up to) 5 created data streams analysers of the OANT instance;
- c) Configuration of OANT to monitor (up to) 1 NIRIS instance endpoints (Networked Interoperable Real-time Information Services endpoints);
- d) Hand-on during the deployment;
- e) Early Life Support (ELS) for 2 weeks after the deployment is finalized;

APP011-2B – OANT Medium Instance:

This flavour provides the required support in deploying (or updating) the OANT Application Service and it consist of:

- a) Deployment of (up to) 5 instance(s) of OANT with (up to) 15 data streams analysers (basic, bidirectional or proxy) based on the protocols supported by the OANT software (see OANT Application Service documentation);
- b) Configuration of the (up to) 15 created data streams analysers of the OANT instance;
- c) Configuration of OANT to monitor (up to) 5 NIRIS instance endpoints (Networked Interoperable Real-time Information Services endpoints);
- d) Hand-on during the deployment;
- e) Early Life Support (ELS) for 2 weeks after the deployment is finalized;

APP011-2C – OANT Large Instance:

This flavour provides the required support in deploying (or updating) the OANT Application Service and it consist of:

- a) Deployment of (up to) 10 instance(s) of OANT with (up to) 25s data streams analysers (basic, bidirectional or proxy) based on the protocols supported by the OANT software (see OANT Application Service documentation);
- b) Configuration of the (up to) 25 created data streams analysers of the OANT instance;
- c) Configuration of OANT to monitor (up to) 10 NIRIS instance endpoints (Networked Interoperable Real-time Information Services endpoints);
- d) Hand-on during the deployment;
- e) Early Life Support (ELS) for 2 weeks after the deployment is finalized;

APP011-3A – OANT Small User Support:

This flavour provides centralised level 2 support to OANT site administrators/users responsible to operate an OANT instance and their level 1 / 3 support organisation.

This flavour enables the support for an already deployed instance of OANT (operations, exercises or demo). It provides expert on-site (or remote) support to administrators, users, trainers and others in the areas of:

- a) Server troubleshooting, configuration and infrastructure integration;
- b) Connection to external data sources;
- c) Data analysis to information issues;
- d) System-to-System interoperability issues;
- e) System Administrator competencies;

It consists of an on-site (or remote) support of up to 2 days (between Monday and Friday), by one technical expert. The expert will work 8 hours a day (working days are exclusive of travel

days). On-site support experts can access a limited amount of back office support in case urgent deeper technical analysis/tests are required on the spot.

APP011-3B – OANT Medium User Support:

This flavour provides centralised level 2 support to OANT site administrators/users responsible to operate an OANT instance and their level 1 / 3 support organisation.

This flavour enables the support for an already deployed instance of OANT (operations, exercises or demo). It provides expert on-site (or remote) support to administrators, users, trainers and others in the areas of:

- a) Server troubleshooting, configuration and infrastructure integration;
- b) Connection to external data sources;
- c) Data analysis to information issues;
- d) System-to-System interoperability issues;
- e) System Administrator competencies;

It consists of an on-site (or remote) support of up to 5 days (between Monday and Friday), by one technical expert. The expert will work 8 hours a day (working days are exclusive of travel days). On-site support experts can access a limited amount of back office support in case urgent deeper technical analysis/tests are required on the spot.

APP011-3C – OANT Large User Support:

This flavour provides centralised level 2 support to OANT site administrators/users responsible to operate an OANT instance and their level 1 / 3 support organisation.

This flavour enables the support for an already deployed instance of OANT (operations, exercises or demo). It provides expert on-site (or remote) support to administrators, users, trainers and others in the areas of:

- a) Server troubleshooting, configuration and infrastructure integration;
- b) Connection to external data sources;
- c) Data analysis to information issues;
- d) System-to-System interoperability issues;
- e) System Administrator competencies;

It consists of an on-site (or remote) support of up to 15 days (between Monday and Friday), by one technical expert. The expert will work 8 hours a day (working days are exclusive of travel days). On-site support experts can access a limited amount of back office support in case urgent deeper technical analysis/tests are required on the spot.

Available on:

NATO Unclassified

NATO Secret

Mission Secret

The Service may be available on other networks upon a New Service Request.

Service Prerequisites: NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side).

Underlying Services: PLT008, INF004

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Trainings not covered by service cost: N/A.

Service Cost/ Price: The cost of service is composed of a Product Life Cycle cost which is a necessary cost to keep the product running regardless of the number of sites running the application, the Product Lifecycle Support unit of measure is unit 1.

There is also a cost for deployment flavours depending on the size of the instance, the unit of measure for these flavours is per instance. There is also a cost for support flavours depending on the requirements of the site, the unit of measure for these flavours is per site.

The cost details are listed in the service rate section of this catalogue release.

APP012 SMACQ Application Service

Service ID: APP012

Service Name: SMACQ Application Service

Portfolio Group: Application Services

Service Description:

The SMACQ (Service to Monitor and Assess Connectivity and Quality) Application Service provides the user with capability to monitor data exchange of operational information dissemination networks to assess and report on its logical connectivity and quality based on Standards. SMACQ leverages and combines information obtained from OANT (APP011) Application Services, to provide further analysis of data quality KPIs, such as connectivity, timeliness, activity and compliancy, insights on historical trends and changes of these KPIs via statistical reports and an overall aggregated graphical view via simple traffic colour-coded indicators.

Value Proposition:

SMACQ Application Service offers the following key benefits for a wide range of users including but not limited to following:

- Commanders, as SMACQ is monitoring and reporting on the full data flow quality, it provides Decision-makers with an enhanced situational awareness and higher increase in the trust on the data they are using to make more effective decisions.
- War fighters (J3 and J6), usually having an isolated, localized view of their data flows, but typically unaware of flows of external data sources, are now able to share a common picture of the data quality, logical connectivity and timeliness of the operational data flow among the battlespace capabilities. SMACQ provides access to simple traffic colour-coded indicators on the systems and services they use, via toggle-able geographical overlays, to improve their situational awareness and trust in the data they are sharing and receiving, so they can be more assured in how they use that data.
- OPS Service Management and Control, SMACQ provides up-to-date web access to the same shared common picture that the war fighters are seeing, with more detailed assessments of the data and connectivity quality indicators, enabling smarter, improved and shared means of monitoring, reporting on connectivity and data quality from source to consumer, to identify, understand and troubleshoot issues in a timely manner.

Service Features:

According to the Bi-SC Operational Requirements for the NATO Common Operational Picture (COP), if the source quality of information data is available, then this shall be accessible to COP users.

SMACQ Application Service provides the following three enhancements to the NATO Common Operational Picture (COP) and Recognized Pictures (RPs) through a toggle-able geo-graphical overlay to the COP/RPs accessible via standardized interfaces (e.g. NVG, KML):

- Source Quality – SMACQ provides knowledge about the source quality, based on Standards-compliance, and potential degradation of the quality for various data flows. For example, the quality of tracks and/or messages generated by a source could be indicated by traffic-light colour-coded dots overlaid on the reported tracks and sources.
- Source Activity – SMACQ provides knowledge about the source activity and how much time had elapsed since that source reported on particular tracks. This is indicated by traffic-light colour-coded lines linking the reported tracks to the sources.
- Source Connectivity – from analysing the data flows from multiple points, the information about a source's logical connectivity, from source to consumer(s), can be inferred and/or extracted, and this information made available to the COP. The source connectivity per source are provided as lines connecting the monitored points from source to consumer(s).
- Data Timeliness – by analysing the data flow activity at each monitored point, the information about data timeliness is also made available to the COP. The data timeliness per connection are indicated by traffic-light colour-coded lines connecting each of the monitored points from source to consumer(s).

The SMACQ Application Service can be offered as a single stand-alone decentralized application service or as a centralized hosted service:

- A centralized hosted SMACQ service can provide insight into an enterprise-level operational network, such as NATO Static Command, to monitor and assess data flows;
- A separate SMACQ application service may provide run-time support during missions and exercises or in a federated-environment, providing localized assessment of those networks, as needed.

Service Flavours:

APP012-1 SMACQ Product Lifecycle Support: This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of the specified application. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year.

APP012-2A – SMACQ Small Instance:

This flavour provides the required support in deploying (or updating) the SMACQ Application Service and it consists of:

- a) Deployment of (up to) 1 SMACQ instance(s) each with up to 2 (already deployed and configured) OANT connections;
- b) Ensuring that the SMACQ picture is represented on (up to) 1 C2 Systems when required (e.g. NCOP, AirC2IS and other systems that support NVG);
- c) Hands-on during the deployment;

- d) Early Life Support (ELS) for 2 weeks after the deployment is finalized;

APP012-2B – SMACQ Medium Instance:

This flavour provides the required support in deploying (or updating) the SMACQ Application Service and it consists of:

- e) Deployment of (up to) 3 SMACQ instance(s) each with up to 5 (already deployed and configured) OANT connections;
- f) Ensuring that the SMACQ picture is represented on (up to) 2 C2 Systems when required (e.g. NCOP, AirC2IS and other systems that support NVG);
- g) Hands-on during the deployment;
- h) Early Life Support (ELS) for 2 weeks after the deployment is finalized;

APP012-2C – SMACQ Large Instance:

This flavour provides the required support in deploying (or updating) the SMACQ Application Service and it consists of:

- a) Deployment of (up to) 5 SMACQ instance(s) each with up to 10 (already deployed and configured) OANT connections;
- b) Ensuring that the SMACQ picture is represented on (up to) 5 C2 Systems when required (e.g. NCOP, AirC2IS and other systems that support NVG);
- c) Hands-on during the deployment;
- d) Early Life Support (ELS) for 2 weeks after the deployment is finalized;

APP012-3A – SMACQ Small User Support:

This flavour provides centralised level 2 support to SMACQ site administrators/users responsible to operate a SMACQ instance and their level 1 / 3 support organisation.

This flavour enables the support for an already deployed instance of SMACQ (operations, exercises or demo). It provides expert on-site (or remote) support to administrators, users, trainers and others in the areas of:

- f) Server troubleshooting, configuration and infrastructure integration;
- g) Connection to external data sources;
- h) Data analysis to information issues;
- i) System-to-System interoperability issues;
- j) System Administrator competencies;

It consists of an on-site (or remote) support of up to 2 days (between Monday and Friday), by one technical expert. The expert will work 8 hours a day (working days are exclusive of travel days). On-site support experts can access a limited amount of back office support in case urgent deeper technical analysis/tests are required on the spot.

APP012-3B – SMACQ Medium User Support:

This flavour provides centralised level 2 support to SMACQ site administrators/users responsible to operate a SMACQ instance and their level 1 / 3 support organisation.

This flavour enables the support for an already deployed instance of SMACQ (operations, exercises or demo). It provides expert on-site (or remote) support to administrators, users, trainers and others in the areas of:

- a) Server troubleshooting, configuration and infrastructure integration;
- b) Connection to external data sources;
- c) Data analysis to information issues;
- d) System-to-System interoperability issues;
- e) System Administrator competencies;

It consists of an on-site (or remote) support of up to 5 days (between Monday and Friday), by one technical expert. The expert will work 8 hours a day (working days are exclusive of travel days). On-site support experts can access a limited amount of back office support in case urgent deeper technical analysis/tests are required on the spot.

APP012-3C – SMACQ Large User Support:

This flavour provides centralised level 2 support to SMACQ site administrators/users responsible to operate a SMACQ instance and their level 1 / 3 support organisation.

This flavour enables the support for an already deployed instance of SMACQ (operations, exercises or demo). It provides expert on-site (or remote) support to administrators, users, trainers and others in the areas of:

- a) Server troubleshooting, configuration and infrastructure integration;
- b) Connection to external data sources;
- c) Data analysis to information issues;
- d) System-to-System interoperability issues;
- e) System Administrator competencies;

It consists of an on-site (or remote) support of up to 15 days (between Monday and Friday), by one technical expert. The expert will work 8 hours a day (working days are exclusive of travel days). On-site support experts can access a limited amount of back office support in case urgent deeper technical analysis/tests are required on the spot.

Available on:

NATO Unclassified

NATO Secret

Mission Secret

The Service may be available on other security domains upon a New Service Request.

Service Prerequisites: NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side).

Underlying Services: PLT008, INF04

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost: N/A.

Service Cost/ Price: The cost of service is composed of a Product Life Cycle cost which is a necessary cost to keep the product running regardless of the number of sites running the application, the Product Lifecycle Support unit of measure is unit 1.

There is also a cost for deployment flavours depending on the size of the instance, the unit of measure for these flavours is per instance. There is also a cost for support flavours depending on the requirements of the site, the unit of measure for these flavours is per site. The cost details are listed in the service rate section of this catalogue release.

APP013 Data-centric Information Services Gateway (DISG) Application Service

Service ID: APP013

Service Name: Data-centric Information Services Gateway (DISG) Application Service

Portfolio Group: Application Services

Service Description: The DISG (Data-centric Information Services Gateway) Application Service provides functional service proxies (FAS Proxy) that support Information Exchange Gateway (IEG) solutions to enable cross-domain exchange of operational data (e.g. Chat, TDLs, JISR, Air, Land, and Maritime). DISG can support IEG-B and IEG-C scenarios (NATO Secret to NATO-Nation Secret enclave, and NATO Secret to NATO-led Mission Secret enclave [reference ADaTP-34 NC3TA Vol. 2 v7, 2005]), which are the most relevant for NATO and partner nations.

Value proposition: Effective operations require the exchange of a wide variety of data within and between Command and Control (C2) systems. The traditional approach to multi-security-domain networking, forbids most information flows crossing the boundary of the security domain. This restrictive approach results in serious limitations to the information exchange requirements among C2 entities. Cross security domain services mediate in any information exchange occurring between the different information domains and levels of classification. The DISG Application Service provides the user with the integration of both Tactical data Link and chat services between distinct security domains, while protecting information assets of the participants in a federated environment.

Service Features: The DISG Service is designed to extend an IEG for Core Services (such as email or web browsing) with extra functionality (in this case with Functional Services). The purpose of DISG are:

- (1) Label – determine and mark the security classification of information passing the IEG, in order to ensure that the information reaches the intended audience,
- (2) Sanitize the information that is intended to leave the security domain. This sanitization will happen according to rules, and it removes or modifies data contents in order to be able to release functional services data into another domain,
- (3) Sign – ensure that data or its security classifications are not changed, by adding digital signatures to the data, when converting data to XML format,
- (4) Verify and guard – ensure the validity of the data by verifying adherence of data to the applicable standards or STANAGs (e.g. STANAG 5516 for Link 16 or XMPP standard for JCHat) both when entering the IEG and when exiting it. Invalid data will not pass the IEG.

The DISG supports multiple formats and protocols, including within the Tactical Data Link (TDL), Message Text Format (MTF), and Chat (XMPP) domains.

- (5) The Diode option is special use case for low to high traffic and provides a way to bridge networks all the way from UNCLASSIFIED to SECRET. It offers a unique

HTTP(S) interface to seamlessly integrate into existing infrastructure. It can also leverage DISG to support the full suite of DISG supported protocols.

The service includes the following activities:

- Support for Incidents and Service request
- Problem management
- Monitoring and Event management (if agreed with Customer and remote access is possible)
- Yearly software upgrade in line with the NCI Agency approved DISG version (A2SL).

Service Flavours:

- APP013-1 Product management: This is the product management for DISG.
- APP013-2A Standard connection – small (per site): connecting up to 5 sites.
- APP013-2B Standard connection – medium (per site): connecting 5-10 sites.
- APP013-2C Standard connection – large (per site): connecting 10+ sites.
- APP013-2D Diode (per site)
- APP013-2E Tailored (custom calculated)
- APP013 – 7 Administrator training (Per training)
- APP013 – 8 Technical Study (Per site)

Available on:

NATO Secret

Availability on any other security domain is TBC upon a New Service Request.

Service prerequisites:

SEC011 Gateway Security Service (If used in a Scenario C case)

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: For the flavours/options where there is a defined unit of measure, a standard service cost is specified. For the Tailored option, the unit of measure is 1, the total of the service delivery cost for these flavours is charged in accordance with specifically arranged conditions of the service delivery.

APP015 JCHAT Application Service

Service ID: APP015

Service Name: JChat Application Service

Portfolio Group: Application Services

Service Description: The JChat (Secure Joint Tactical Chat) Application Service provides the user with a federated chat network to allow near real-time communication, or semi-synchronously via text messages, between two users, ad-hoc groups and within persistent chat rooms.

Value Proposition: The JChat Application Service is a key component in facilitating military effectiveness. It enables passing of information, coordination of operations and support to collaborative decision making. The service focuses on time critical operations in order to prevent casualties and minimise reaction time.

Service Features: The JChat Application Service key features include but are not limited to:

- Multi-party messaging service (ad-hoc and persistent chat rooms)
 - Within a mission network, chat applications are used in a similar manner to Combat Net Radio, allowing all-informed exchange of information within specific groups or chat rooms.
 - Chat rooms are used both informally, for staff level coordination and collaboration, and formally, for rapid all-informed reporting and tasking.
- One-to-one messaging service (chat sessions)
 - Presence and instant messaging (IM) defines a method by which a client or user can formally request establishment of a presence and instant messaging session.
 - The functionality of the JChat Application Services follow open standards and are set in conformance with the requirements in RFC 2779 ("Instant Messaging / Presence Protocol Requirements").
- Roster service (contact list)
 - In JChat, a user's roster contains any number of specific contacts. A user's roster is stored by the user's server on the user's behalf so that the user can access roster information from any device.
 - Because the user's roster can contain confidential data, the JChat server restricts access to this data so that only authorized entities (typically limited to the account owner) are able to retrieve, modify, or delete it.
- Presence service (logged-on users)
 - The concept of presence refers to an entity's availability for communication over a network.

Service Flavours:

The service has the following flavours:

Service flavour name	Unit
APP015-1 JCHAT Product Lifecycle Support	1
APP015-2A JCHAT Small Instance (Up to 200 Users)	Per Instance
APP015-2B JCHAT User Support Small (up to 200 Users)	Per User Site
APP015-3A JCHAT Medium Instance (Up to 2000 Users)	Per Instance
APP015-3B JCHAT User Support Medium (Up to 2000 Users)	Per User Site
APP015-4A JCHAT Large Instance (Up to 4000 Users)	Per Instance
APP015-4B JCHAT User Support Large (Up to 4000 Users)	Per User Site

Available on:

NATO Secret
Mission Secret

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9005	JChat M-Link Server Administrator
A9006	JChat Combined Openfire Server and JChat Client Administrator

Service Cost / Price:

The cost of service is composed of a product life cycle support cost, which is a necessary cost to keep the product running regardless of the number of sites running the application;



the product lifecycle support unit of measure is 1. There is also a cost for deployment and support flavours depending on the size of the site. The unit of measure for these flavours is per instance and per site respectively. The cost details are listed in the service rate section of this catalogue release.

APP016 JTS/FAST Application Service

Service ID: APP016

Service Name: JTS/FAST Application Service

Service Type: Customer Facing

Portfolio Group: Application Services

Service Status: Available

Service Description: The JTS-FAST (Joint Targeting System/Functional Area Service for dynamic and time-sensitive Targeting) Application Service provides the user with capabilities to provide integrated joint objective and effects-based targeting, campaign synchronisation, target development, target list management, target folder preparation, target imagery management and battle damage assessment.

Value Proposition: The JTS-FAST Application Service, used throughout all command levels in NATO (both static and deployed) as well as nationally by various nations, enables collaboration and the efficient and timely exchange of critical information in support of the Joint Targeting process. Furthermore this service is designed to aid tracking and prosecuting of Time-Sensitive Targeting (TSTs).

Service Features: The JTS-FAST Application Service contains multiple end user modules, with distinct features:

- JTS features:
 - Deliberate Targeting
 - Kinetic and Non-Kinetic Targeting
 - Effects-Based Targeting (JFX)
 - High Value Individual (HVI)
 - Target Development
 - Target Folder Preparation
 - Objective Management
 - Target List Management
 - Target Nomination Process
 - Target Media Management
 - Weaponing Solutions
 - Battle Damage Assessment (BDA)
 - Campaign Synchronization
 - ATO Planning Cycle
- FAST features:
 - Dynamic Targeting (DT)
 - Time-Sensitive Targeting (TST)
 - Integrated Chat capability
 - Integrated Map functions

- Network-enabled, real-time coordination
- JTSLink features
 - JTS database replication
- JTSDBAAdmin features
 - JTS database administration
- JTSWISI
 - JTS NVG web services

Service Flavours: The service is available in multiple flavours.

Flavour #	Flavour Name
APP016-1 JTS-FAST Product Lifecycle	1
APP016-2A JTS-FAST Small Instance	Per Instance
APP016-2B JTS-FAST Medium Instance	Per Instance
APP016-2C JTS-FAST Large Instance	Per Instance
APP016-3A JTS-FAST User Support Small	Per User Site
APP016-3B JTS-FAST User Support Medium	Per User Site
APP016-3C JTS-FAST User Support Large	Per User Site

Available on:

- Any network of customer
- NATO Secret
- Mission Secret, VeVA

Service Prerequisites: Infrastructure compatible with the requirements of the application as described in the release documentation.

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1007	JTS/FAST System Administrator Course
A9008	Functional Area Service for dynamic and time-sensitive Targeting (FAST) User Course
A9011	Joint Targeting System (JTS) User Course
A9073	JTS/FAST Combined User Course
A9074	JTS/FAST Data Manager Course

Service Cost / Price:

The cost of service is composed of a product life cycle support cost which is a necessary cost to keep the product running regardless of the number of sites running the application, the product lifecycle support unit of measure is unit 1. There is also a cost for deployment and support flavours depending on the size of the site. The unit of measure for these flavours is per instance and per site respectively. The cost details are listed in the service rate section of this catalogue release.

APP017 Land C2 Application Service

Service ID: APP017

Service Name: Land C2 Application Services

Service Type: Customer Facing

Portfolio Group: Application Services

Service Description

The Land Command and Control (C2) Application Services provides a suite of land command and control applications that support operational land staff in decision making and execution of missions, processes and tasks.

The Land C2 Application Services delivers comprehensive situational awareness, battlespace management, sharing of information and interoperability within the land C2 domain and between other NATO functional services and national land C2 capabilities.

Value Proposition

The Land C2 Application Services, through SitaWare Headquarters (HQ), offers a wide range of features to the user including shortened information-decision-action (IDA) cycles, inherent to command and control of mission execution. The service enables:

- Effective, efficient and accurate management of recognized ground picture (RGP);
- Enhanced battlespace management;
- Integrated situational awareness;
- Support for operations planning and FRAGO production and message generation;
- Sharing of recognized ground picture, information and knowledge;
- Automated importing of recognized ground picture contributions and messages.

The services ranges from centralised management of land C2 application licenses, export authorisations and vendor logistics support, to the sustainment of the land C2 application services within headquarters through the provision of in-service support.

Service Features

The main service consists in the provision of the following service features:

- **Access to Land C2 Application Service** and related resources on selected networks and to the technical and functional knowledge base for self-support (requires access to the NCI Agency managed Operational Network).
- **Site Installation and Activation** provides on-site installation of one Land C2 application service instance and connection to all compatible and pre-configured local sources at time of installation.

- **Management and In-Service Support** provides centralised management and maintenance of the Land C2 capabilities and site installations, including assistance and support to local support engineers. It includes deployment and activation of routine upgrades and patches as become available in line with the approved baseline. For fully centralised management, remote administrator access is required.
- **Remote Support** provides centralised assistance and advice to local support engineers who maintain the local Land C2 application service. It includes support to deployment and activation of routine upgrades and patches as become available in line with the approved baseline. This option is available when no remote administrator access is feasible or required.
- **Incidents and Service Requests Management** provides centralised support to resolve incidents and/or address service requests via ITMS ticketing system to log, categorize and escalate if applicable. Response time and level of response in accordance with defined service level agreement.
- **Problem Management** to identify and manage the underlying causes of incidents and prevent them from occurring again.

The service includes the following application assets:

- **SitaWare Headquarters:** NATO currently manages 500 SitaWare HQ user licenses, distributed over the various sites.

The standard configuration per site will consist of one operational instance and one training/exercise instance.

LC2IS support will be discontinued from 2026 onwards; extended (limited) support may be offered on specific customer request.

Service Flavours

APP017-1 SitaWare HQ Product Lifecycle Support – This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of SitaWare HQ regardless of the number of sites using the product. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year. The product lifecycle support unit of measure is unit 1.

APP017-2 SitaWare HQ Standard Instance – This flavour provides for a single running copy (instance) of SitaWare HQ on specified network domain with its own specific setup, configuration and user access. This includes the prerequisite hosting infrastructure and platform of the instance on specified network domain, the maintenance and support for the infrastructure, platform and running instance, such as OS upgrades, application upgrades and hot-fixes, and backup and recovery management during one year.

APP017-3A SitaWare HQ User Support Small Site (1-75 Users) – This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 75 users. The flavour includes provision of centralized technical support, incident

management, request fulfilment, access management, and problem management during one year.

APP017-3B SitaWare HQ User Support Medium Site (76-200 Users) – This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 200 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.

SitaWare HQ User Support Large Site (200> Users) (Custom Rate) – This custom flavour offers the same services as flavour APP017-04 for sites with over 200 users.

SitaWare HQ User License (new or additional) (Custom Rate) – This custom flavour is for the procurement of new or additional licenses of SitaWare HQ. This flavour does not include implementation and follow-on in-service support.

SitaWare HQ Instance Deployment (Custom Rate) – This custom flavour is for the deployment of one instances of SitaWare HQ at a network domain.

SitaWare HQ New Site Early-life Support (Custom Rate) – This custom flavour is offers early-life support during implementation of a site.

SitaWare HQ On-Site Support (Custom Rate) – This custom flavour offers on-site functional and/or technical support.

SitaWare HQ Exercise Support (Custom Rate) – This custom flavour offers functional and/or technical support during an exercise above and beyond the support already covered within CSLA.

Available On

- NATO Secret;
- Mission Secret;
- VeVA;
- Deployable CIS.

The application service may be made available on other security domain/networks which will be assessed upon a new customer service request.

Service Prerequisites

- NDW002 NATO Digital Workplace Service (High Side) - for application instances installed on NCI Agency managed networks);
- INF004 Infrastructure Virtualization Service: for infrastructure and hosting platform compatible with the Land C2 Application Services requirements;
- PLT006 Database Platform Service: Database platform compatible with the Land C2 Application Services requirements;
- APP055 - Core GIS: for Open Geospatial Consortium (OGC) compliant map services.

Standard Service Support Levels

- **Service Availability Target:** 99.5%
- **Service Restoration:** This service is included as critical service, the service restoration period for widespread outage within NCS is 8 hours Wall Clock (P2+), otherwise a lower priority will be assigned.

N.B.1: Availability and restoration times of the Land C2 application services are primarily dictated by the availability of the underlying services.

N.B.2: Full priority resolution times and generic service priority assignment matrix will be adhered to in accordance with the defined service level agreement.

Service Reporting: Periodic reporting as agreed with the customer.

Training

SitaWare HQ training will be offered by the NCI Academy; for available courses, please refer to NCI Academy training catalogue. Provision of training is not covered by the service rate.

Service Cost / Price

The cost of the service is composed of a product life cycle support cost, which is a necessary cost to keep the product running regardless of the number of sites running the application; the product lifecycle support flavour unit of measure is 1. There is also a cost for deployment and support flavours depending on the size of the site, the unit of measure for these flavours is per instance and per site respectively. The cost details are listed in the service rate section of this catalogue release, except for the “custom” flavours. For the “custom” flavours, the unit of measure is 1 at a custom rate.

.

APP018 Maritime C2 Application Service

Service ID: APP018

Service Name: Maritime C2 Application Service

Service Type: Customer Facing

Portfolio Group: Application Services

Service Status: Available

Service Description: Maritime Command and Control (C2) Application Service consists of a number of instantiations of the Maritime C2 Information System (MCCIS) Version 7, which is a product of Northrop Grumman UK Limited (NGUKL), used as the NATO's main Maritime C2 Capability.

MCCIS processes maritime data received from Nations, builds the NATO Recognized Maritime Picture (RMP), incorporates White Shipping Picture (WSP) data, displays the RMP on a map, and disseminates the RMP to Nations, NATO Commands, and other C2 applications. MCCIS provides the operational users with maritime operational data, exchanged in a multi-national environment through Over the Horizon Targeting (OTH-T GOLD) messages and Allied Data Publication No.3 (ADatP-3) messages from APP-11.

MCCIS also provides the Waterspace Management (WSM) and Prevention of Mutual Interference capabilities to Command Submarines of NATO (COMSUBNATO) to support subsurface mission space management.

MCCIS has a Client-Server architecture. The infrastructure components are given below:

Server: MCCIS server, virtualised on the deployment site

Standard Clients: NATO standard client machines (thin clients) available on site

Special Clients: Special positions to use client hardware (personal computers).

The main software components are given below:

Integrated Command Control Services (ICS)

Waterspace Management (WSM) Module

Common Operational Picture (COP) Synchronisation Tool (CST).

Depending on the purpose and site, following MCCIS Server Groups are available:

HQ MARCOM RMP Servers

HQ MARCOM WSP Servers

HQ MARCOM COMSUBNATO Servers

National Gateways (National enclaves)

Standing Naval Forces (SNF) Afloat Command Platforms (provided by APOLLO Kits)

Collective Training

Individual Training

Exercise

Mission Network.

Value Proposition: MCCIS provides the user with management of Maritime C2 information received from multiple sources. MCCIS can receive, process, display, and share Maritime C2 information. It supports operational planning, maritime situational awareness, and subsurface mission space management. These key capabilities provide support to the maritime commanders and HQ staff to conduct NATO maritime operations with more accurate and timely decisions.

Service Features: The Maritime C2 Application Service has the following features:

- Receiving track data from Nations;
- Receiving White Shipping Picture data from unclassified data sources;
- Processing track data from multiple sources, performing correlation, and identifying ambiguities;
- Building the NATO RMP;
- Displaying the NATO RMP over a map in user-defined form;
- Supporting the users to perform Maritime Situational Awareness;
- Supporting the COMSUBNATO to perform WSM;
- Sharing the NATO RMP with the MCCIS gateways located at national enclaves (Nations are expected to provide data to these gateway or receive data from them);
- Sharing the NATO RMP with other MCCIS servers in other NATO Commands;
- Providing the NATO RMP with the MCCIS server on board the NATO Command Ships (using CST function of MCCIS running one SNF Kits);
- Providing NATO RMP to any NATO ship having MCCIS on board;
- Enabling the HQ staff to exchange APP-11 messages.

The NATO Maritime C2 Capability comprises a number of MCCIS servers to enable the above features. The Application Service provides support and maintenance to the C2 of Maritime Operations at enterprise level.

Provision of service is unchanged as MCCIS remains as the main NATO Maritime C2 Information System.

Service Ordering and Request: The Application Service provides standard support to ACO. In addition, Nations may have their own MCCIS servers, at static or afloat sites, which they can use for national purposes. This Application Service does not cover the support to Nations, but includes coordination of any maintenance requests with ACO.

Service Flavours: This Service has the following flavours:

- APP018-1 Product Lifecycle Support (for the entire NATO Maritime C2 Capability)
- APP018-2 Instance (costs for one MCCIS7 instance; detailed costs to be determined according to site capabilities and operational requirements).

Available on:

NATO SECRET

Service Prerequisites:

INF004 Infrastructure Hosting Service

NDW002 NATO Digital Workplace Service (High Side)

Standard Service Support Levels:

Service Availability¹ Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting: Through ITSM.

Available NCI Academy Training (not covered by Service Cost):

A0270	NATO MCCIS Orientation & User
A0271	NATO MCCIS RMP Operator
A0273	NATO MCCIS Site Administrator
A0275	NATO MCCIS Waterspace Management
A0277	NATO MCCIS RMP Supervisor
A0602	Maritime FAS Pre-study (013)
A0603	MCCIS Pre-study (014)
A0609	MCCIS Advanced (031)

Service Cost / Price:

The cost of service is composed of a Product Lifecycle Support cost, which is necessary to keep the product running regardless of the number of sites running the application. The Product Lifecycle Support unit of measure is 1.

There is also a cost for the initial setup of one MCCIS instance; the unit of measure for this flavour is per instance.

The cost details are listed in the service rate section of this catalogue release.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

APP021 JOCWatch Application Service

Service ID: APP021

Service Name: JOCWatch Application Service

Portfolio Group: Application Services

Service Description: JOCWatch is Web application, created to provide a common web-based interface to allow a Headquarters (HQ) staff, such as those in at Combined Joint Operations Centre (CJOC) in the NATO missions, to manage, analyse and publish information on incidents of relevance reported to that command. JOCWatch provides HQ staff with:

- An electronic event log enabling the capturing and recording of incident information including time of incident, location, casualty data and other relevant details.
- A way to import incidents from federated incident reporting systems (either other JOCWatch instances or other NATO incident reporting systems) enabling the maintenance of data consistency and maintaining references to the originating source.
- An audit of the incidents in the campaign, showing the information that was available to the HQ at any time – and who entered it. Following the end of the operation the JOCWatch incident data log entries can form part of the Commander's Diary or Official Operational Record that is archived within national historical records repositories as well as central records archive at SHAPE.
- A managed data source as the foundation of an up-to-date incident report for a Common Operational Picture (COP).

Value proposition: The JOCWatch Application Service offers a wide range of support to entities willing to make permanent or temporary use of JOCWatch in their static and/or deployed environment. The proposed services ranges from the implementation of an JOCWatch instance through to corrective maintenance, including training and mentoring of operational and support personnel, as well as centralised resources and support for handling service degradation or interruption.

Service Features:

- **Service Delivery Point (SDP) activation** provides on-site installation of one JOCWatch instance including instance configuration and customization according to mission requirements
- **SDP Remote Support** provides centralised assistance and advice to local Support Engineers who maintain the JOCWatch SDP and includes up to one on-site upgrade in line with the approved baseline. By default, includes 12 tickets with a maximum response time of 5 business days. No remote administrator access required.
- **SDP Management** includes “SDP Remote Support” and complements with a local footprint for technical support. Remote administrator access required.
- **Service Access Point (SAP) activation** provides configuration of on-site user access to an existing JOCWatch SDP. It includes combined training from JOCWatch User through to JOCWatch data manager, as well as knowledge transfer for 2 Support

Engineers to act as first responder for Incidents and Service Requests and interface with the Agency Support.

- **SAP Remote Support** provides centralised assistance and advice to resolve incidents and/or address service requests via NATO/NCIA ITSM ticketing system to log, categorize and escalate if applicable. By default, includes 12 tickets per SAP. No remote power-user access is required.
- **SAP Management** includes “SAP Remote Support” and complement with a local footprint for functional/technical advice as well as technical liaison with the SDP management and assistance in recording and handling incidents and/or service requests via NATO/NCIA ITSM ticketing system. Remote power-user access required.

Service Flavours: The service is available with the following flavours:

APP021-1 JOCWatch Product Lifecycle: This service flavour provides centralized application maintenance and availability of the JOCWatch service for the Bi-SC and for ACO exercises planning cycle for the current year.

APP021-2 JOCWatch for an Organizational Entity (NCS-A) or NATO Mission: This service flavour provides full JOCWatch usage for an Organisational Entity (NCS) or NATO mission. It includes three instances in the Service Delivery Point; operational, exercise and training. The support is planned up to 200 users. It includes remote and on-site mentoring.

APP021-3 JOCWatch for a Federated Entity: This service flavour provides federation support to NFS and Nations for authorization, configuration and troubleshooting of their connections to an JOCWatch Service Delivery Point (identified as centralized NCS Col servers).

This flavour also encompasses Application changes triggered by federation requests and compensation for capacity increase required by the increasing demand on corresponding centralized infrastructure.

Types of possible federations are:

B2C: remote connection to centralized SDP (up to 20 users)

B2B: synchronisation connection to centralized SDP

E2E: managed sessions to centralized SDP (up to 20 sessions)

This service flavour ensures initialization and continuity of the COI interconnections between Nations & NFS with NCS. Troubleshooting beyond NATO Interconnection Point on the national or NFS side is not included in this service flavour. The service flavour offers:

- Management of technical connectivity to centralized NCS COI servers given the requester has authorization from SHAPE and the corresponding NCS party
- Troubleshooting on configuration of the connection to centralized NCS COI servers
- Application service delivery monitoring & corrective actions
- Application changes triggered by this federation request

- Compensation for capacity increase as per the increasing demand on corresponding NCS Col servers

ICT support services to External Customers is recommended to complement this flavour, would the Customer have connectivity in B2B mode. This is recommended for support beyond NIP.

APP021-4 JOCWatch Additional Instance for Existing Organizational Entity: This service flavour provides additional instance next to existing NCS or FED ones.

APP021-5 JOCWatch in a NATO Exercise: This service flavour provides standard exercise planning and execution support for NATO exercises. It includes exercise design review, dedicated exercise configuration, on-site application management, and after-action analysis report for any NATO exercise. Planning excluded (already included in Product Lifecycle flavour)

Available on:

All NATO and National networks

APP021-3: NATO Secret

Service prerequisites: Infrastructure compatible with the requirements of the JOCWatch application as described in the Release documentation.

APP021-FED: Network connectivity for NIP interconnection with NATO centralized network (NS).

Underlying Services: INF004, INF005, INF007, INF016, PLT006, PLT008, OTH001, SME005

Standard Service support levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Available NCI Academy Training not covered by service cost:

A9031	NATO JOCWatch Power User
A9035	NATO JOCWatch Administration

Service Cost / Price: The unit of measure for the Service is 1 for APP021-1 flavour.

For APP021-2, the unit of measure is the site utilizing the service (per site).

For APP021-3, the unit of measure for the Service is per connection.

For APP021-5, the unit of measure is the exercise where the service is used (per event).

The price details for each of the service flavours is specified in the Costed Customer Service Catalogue (CCSC).

APP022 NCOP Application Service

Service ID: APP022

Service Name: NCOP Application Service

Portfolio Group: Application Services

Service Description: The NCOP (NATO Common Operational Picture) application provides operational user with a common view of the battle space. NCOP is interoperable with a large set of NATO and National Systems, collating and harmonizing authoritative information into Common Operational Pictures (COP) tailored for a mission or an area of interest, thus enabling a timely execution of operational users' processes (Battlespace Management, Logistics, Targeting, MEDEVAC, etc).

Furthermore, the NCOP Application Service also contributes to the Ballistic Missile Defense capability through integration of specific functions and interfaces for BMD.

Value proposition: The NCOP Application Service offers a wide range of support to entities willing to make permanent or temporary use of NCOP in their static and/or deployed environment. The proposed services ranges from the implementation of an NCOP instance through to corrective maintenance, including training and mentoring of operational and support personnel, as well as centralised resources and support for handling service degradation or interruption.

Service Features:

- **Access to NATO Common Operational Picture** application and related resources through the NCI Agency DML (under license agreement) and to technical and functional Knowledge Base (NCOP Support Portal) for self-support (requires access to the Agency managed Operational Network).
- **Service Delivery Point (SDP) activation** provides on-site installation of one NCOP instance and connection to all compatible and pre-configured local sources at time of installation. Includes training of up to 3 COP managers (see NCI Academy ref. A9047 for details) and access for users through the Activation of Service Access Point feature (1 unit is included) for a maximum of 3 SAP for the same SDP.
- **SDP Remote Support** provides centralised assistance and advice to local Support Engineers who maintain the NCOP SDP and includes up to one on-site upgrade in line with the approved baseline. By default, includes 12 tickets with a maximum response time of 5 business days. No remote administrator access required.
- **SDP Management** includes "SDP Remote Support" and complements with a local footprint for technical support. Remote administrator access required.
- **Service Access Point (SAP) activation** provides configuration of on-site user access to an existing NCOP SDP for up to 24 users to consume a shared COP. It includes combined training from COP User through to COP Contributor for up to 24 users (see NCI Academy ref. A9054 for details), as well as knowledge transfer for 2 Support

Engineers to act as first responder for Incidents and Service Requests and interface with the Agency Support.

- **SAP Remote Support** provides centralised assistance and advice to resolve incidents and/or address service requests via NATO/NCIA ITSM ticketing system to log, categorize and escalate if applicable. By default, includes 12 tickets per SAP. No remote power-user access is required.
- **SAP Management** includes “SAP Remote Support” and complement with a local footprint for functional/technical advice as well as technical liaison with the SDP management and assistance in recording and handling incidents and/or service requests via NATO/NCIA ITSM ticketing system. Remote power-user access required.

Service Flavours: The service is available with the following flavours:

APP022-1 NCOP Product Lifecycle Support: This service flavour provides centralized application maintenance and availability of the NCOP service for the Bi-SC and for ACO exercises planning cycle for the current year.

APP022-2 NCOP for an Organizational Entity (NCS-A) or NATO Mission: This service flavour provides full NCOP usage (including COP management) for an Organisational Entity (NCS) or NATO mission. It includes three instances in the Service Delivery Point; operational, exercise and training. The support is planned up to 200 users. It includes remote and on-site mentoring.

APP022-3 NCOP Access-Only for an Organizational Entity (NCS-A): This service flavour provides limited NCOP usage (excluding COP management) as access-only for an Organisational Entity (NCS). It includes two instances in the Service Delivery Point; operational and exercise. The support is planned up to 50 users. It includes remote mentoring only.

APP022-4 NCOP for a Federated Entity: This service flavour provides federation support to NFS and Nations for authorization, configuration and troubleshooting of their connections to an NCOP Service Delivery Point (identified as centralized NCS Col servers).

This flavour also encompasses Application changes triggered by federation requests and compensation for capacity increase required by the increasing demand on corresponding centralized infrastructure.

Types of possible federations are:

B2C: remote connection to centralized SDP (up to 20 users)

B2B: synchronization connection to centralized SDP

E2E: managed sessions to centralized SDP (up to 20 sessions)

This service flavour ensures initialization and continuity of the COI interconnections between Nations & NFS with NCS. Troubleshooting beyond NATO Interconnection Point on the national or NFS side is not included in this service flavour. The service flavour offers:

- Management of technical connectivity to centralized NCS COI servers given the requester has authorization from SHAPE and the corresponding NCS party
- Troubleshooting on configuration of the connection to centralized NCS COI servers
- Application service delivery monitoring & corrective actions
- Application changes triggered by this federation request
- Compensation for capacity increase as per the increasing demand on corresponding NCS COI servers

ICT support services to External Customers is recommended to complement this flavour, would the Customer have connectivity in B2B mode. This is recommended for support beyond NIP.

APP022-5 NCOP in a NATO Exercise: This service flavour provides standard exercise planning and execution support for NATO exercises. It includes exercise design review, dedicated exercise configuration, on-site application management, and after-action analysis report for any NATO exercise. Planning excluded (already included in Product Lifecycle flavour)

APP022-6 NCOP in a large NATO Exercise: This service flavour provides large-scale exercise planning and execution support for NATO exercises. It includes exercise design review, dedicated exercise configuration, on-site application management, dedicated reach-back expertise up to Level 4 and after-action analysis report for any NATO exercise. Planning excluded (already included in Product Lifecycle flavour)

Available on:

All NATO and National networks

APP022-4: NATO Secret

Service prerequisites: Infrastructure compatible with the requirements of the NCOP application as described in the Release documentation.

APP022-4: Network connectivity for NIP interconnection with NATO centralized network (NS).

Underlying Services: INF004, INF005, INF007, INF016, PLT006, PLT008, OTH001, SME005

Standard Service support levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Available NCI Academy Training not covered by service cost:

A9046	NATO Common Operational Picture (NCOP) User
A9047	NATO Common Operational Picture (NCOP) COP Manager

A9048	NATO Common Operational Picture (NCOP) Combined User and COP Manager
A9049	NATO Common Operational Picture (NCOP) FAS Administrator
A9050	NATO Common Operational Picture (NCOP) System Administrator
A9051	NATO Common Operational Picture (NCOP) Combined COP Manager and FAS Administrator
A9053	NATO Common Operational Picture (NCOP) Train the Trainer Operational User

Service Cost / Price: The unit of measure for the Service is 1 for APP022-1 flavour.

For APP022-2 and APP022-3, the unit of measure is the site utilizing the service (per site).

For APP022-4, the unit of measure for the Service is per connection.

For APP022-5 and APP022-6, the unit of measure is the exercise where the service is used (per event).

The price details for each of the service flavours is specified in the Costed Customer Service Catalogue (CCSC).

APP023 NAMIS Application Service

Service ID: APP023

Service Name: NAMIS Application Service

Portfolio Group: Application Services

Service Description: NATO Automated Meteorological Information System (NAMIS) Application Service provides a sustained NATO Meteorological and Oceanographic (METOC) application functionality for the NATO. NAMIS Application Service provides direct weather support to NATO-led operations by providing coherent, comprehensive, and harmonised weather information and products throughout ACO activities.

Value Proposition: The NAMIS Application Service delivers METOC information to its users, principally within two Communities of Interest groups; MetOc and Ops Communities. NAMIS Application Service enables the user to access raw MetOc data and able to produce MetOc observations. Those can be used to support Exercise or Operation planning, Navigation, Natural Hazard Prevention/Analysis, Logistic Support Planning, Air/Missile Defence Operation planning/analysis, Weather Forecast Impact Analysis purposes. Users can also visualise all available MetOc products and data via NAMIS. Thus, interoperability of weather systems and other FAS is enabled.

Service Features: The NAMIS Application Service provides below listed features:

- Provision of Environmental Information Products,
 - MetOc Data Distribution System
- Meteorological Assessment,
 - visualization of forecasts,
 - visualization of observations,
 - visualization of value added products such as satellite images,
 - management of information on meteorological stations
- Tactical Specialist Tools,
 - Meteorological messages for CBRN (EDM and CDM),
 - Ballistic Wind Messages,
 - Color state and forecast trend for user selected airfields (METWATCH),
 - Products supporting parachute operations Mean Effective Dropping Wind (MEDW), Surface Wind and Gusts (SFG),
 - Theatre Crosswind Monitor, to monitor selected airfield for crosswind threshold,
 - Density Altitude calculator to verify conditions for use of air assets on the specific areas,
 - Graphical depiction of "Human Exposure", including Temperature-Humidity index (Heat Stress), Wind-Chill, Cold-Water Survival,
 - Night Illumination.
- Operational Planning Support (meteorological briefs in support of operations);
- Meteorological briefs in support of operations.

Service Flavours: The NAMIS Application Service is available as three flavours; namely:

- NAMIS X Premium; Superior license type providing full suite of full MetOc analysis tools
- NAMIS Basic; junior license type providing access to limited MetOc analysis capability
- NAMIS 'NATO MetOc (NMD) Web Portal providing access to...MetOc information

Available on:

NATO Secret
NATO Unclassified
Mission Domains

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: PLT008, OTH001, SME005

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP025 Naval Mine Warfare Support Application Service

Service ID: APP025

Service Name: Naval Mine Warfare Support Application Service

Portfolio Group: Application Services

Service Description: The Naval Mine Warfare Support Application Service consists of MCM EXPERT, which is a tool used for planning Naval Mine Counter Measure (MCM) operations to achieve user-specified level of clearance of maritime channels through uniform and non-uniform coverage according to the doctrine stipulated in STANAG 1454. The service is used on standalone computers at operational-level NATO sites and on board MCM vessels at tactical level.

Value Proposition: The Naval Mine Warfare Support Application Service offers the user a Graphical User Interface (GUI) for interactive planning of MCM operations. Based on the user inputs for a number of MCM operation types, MCM EXPERT provides the user a response in the form of a set of minesweeping or mine hunting tracks, with specific placement across the channel, and the clearance and remaining risk level achieved after completion of the given plan.

Service Features: The Naval Mine Warfare Support Application Service provides the ability to build Uniform and Non-Uniform MCM plans based on level of clearance, remaining risk, and Non-Uniform plans for time-constrained operations. Metrics of clearance, and remaining risk, achievable with the selected plan presented to the user.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side).

Underlying Services: PLT008, OTH001

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP026 Virtual Battle Simulation (VBS) Application Service

Service ID: APP026

Service Name: Virtual Battle Simulation (VBS) Application Service

Portfolio Group: Application Services

Service Description: The Virtual Battle Simulation (VBS) application service supports an exercise control organisation in maintaining a virtual situation of the battle space consistent in time and space at the level of detail of individual actors with a degree of realistic visualisation.

The VBS application is a commercial-off-the-shelf immersive training application used to simulate a real-time video stream. It functions as stand-alone or connected to the JCATS model.

Value Proposition: This application service supports exercise designers and control organisations in generating life-like visualizations of the relevant battlespace.

Service Features: The Virtual Battle Simulation (VBS) application service offers the following features:

- Creation and modification of a virtual scenario including terrain, systems and personnel. Activities of systems and personnel can be pre-planned and previewed.
- A player and controller mode to execute the scenario and act as one the parties or as the scenario manager.
- Video capture to mimic the behaviour of real-time optical or infra-red sensors.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side).

Underlying Services: OTH001

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.



APP027 NATO Nuclear C2 Reporting Application Service

The Service is classified. Further information is available upon request and relevant clearance.



APP028 NATO Nuclear Planning Application Service

The Service is classified. Further information is available upon request and relevant clearance.

APP029 Military Message Handling Application Service

Service ID: APP029

Service Name: Military Message Handling Application Service

Portfolio Group: Application Services

Service Description: Military Message Handling Application Service provides the user, in both static and deployed environments, with the capability of drafting, releasing and receiving military messages (ACP127 and X400). The service also delivers a reliable message storing and forwarding infrastructure, which provides intercommunication between NATO organisations, Maritime Broadcast systems and National ACP127 networks.

Value Proposition: Military Message Handling Application Service offers the customers:

- The intercommunication between NATO and National Military Organizations,
- The automatic distribution of incoming and outgoing formal military messages based on information within a message and rules following the operational and administrative procedure,
- A sequential/parallel workflow capability to support the coordination of message preparation.

Service Features: The Military Message Handling Application Service offers features:

- Integrated Messaging Application (Web-based or desktop application)
- Address Book
- Message Attachments
- Digital Signature (at server level)
- ADat-P3 Integration
- Central Archive
- Access Management
- Alternate Recipients
- Deferred Delivery
- Enhanced Message Reporting and Notifications (Read/ Delivered/Deleted)
- Computer Based User Training (JADL Platform – ADL 126 – XOmail Messaging)
- Message Templates Management
- Message Security Labelling
- Information Exchange Gateways (ACP127 and SMTP-RFC6477)
- Quality of Service adjustments based on different message priorities (e.g. expediting higher priority messages)

Service Flavours: The Military Message Handling Application service is available in multiple flavours:

- APP029-1 MMHS Product Lifecycle Support: This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of the specified application. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and

knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year.

- APP029-2 MMHS Instance: This flavour provides for a single running copy (instance) of an application on specified network domain with its own specific setup, configuration and user access. This includes the hosting infrastructure and platform of the instance on specified network domain, the maintenance and support for the infrastructure, platform and running instance, such as OS upgrades and application upgrades and hot-fixes, and backup and recovery management.
- APP029-3 MMHS User Support Small: This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 300 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.
- APP029-4 MMHS User Support Medium: This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 1000 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.
- APP029-5 MMHS User Support Large: This flavour offers user access management and user support for all levels of users. The flavour applies to one site with more than 1000 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.
- APP029-6 MMHS Message Operator Support (former SME010): This flavour includes the activities related to the 24/7 formal/military message service operations and support to NCIA External Customers; in more details: provision of message organizations (aka SMA/PLA) and message distribution, timely delivery of sent/received military messages, address book management.

Available on:

NATO Secret
Mission Secret
VeVA

Service Prerequisites:

INF002 - NATO Network Point of Presence
NDW002 NATO Digital Workplace Service (High Side)
WPS012 E-mail Services

Underlying Services: PLT008, OTH001, SME005, TRA002, INF004, PLT015

Standard Service Support Levels:

Service Availability Target: 99.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price:

The cost of this service is composed of a product life cycle support cost which is a necessary cost to keep the product running regardless of the number of sites running the application, the product lifecycle support unit of measure is unit 1 . There is also a cost for deployment and support flavours depending on the size of the site, the unit of measure for these flavours is per site . The cost details are listed in the service rate section of this catalogue release .

Available NCI Academy Training not covered by service cost:

A0160	Allied Information Flow System (AIFS) Administrator
A0161	Allied Information Flow System (AIFS) Operator/Shift Supervisor
A0162	New NATO Messaging System (NNMS) Message Service Operator



APP030 Tasker and Project Tracker Applications Service (TT+ and PITT)

Service transitioned to NDW006.



APP031 Enterprise Document Management Application Service (EDMS)

Service transitioned to NDW006.

APP032 Personnel Management Application Services

Service ID: APP032

Service Name: Personnel Management Application Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Available

Service Description: The Personnel Management Application Service is supporting the Human Resource community by providing users with tools and systems for supporting day-to-day operational activities such as Personnel, Jobs, and Organization Management for the NATO static and deployed Command Structure. The Service enables the user to access, collect, store, manage, analyse, present, process, and disseminate human resource information.

Value Proposition: The Service offers the user improved accuracy, relevance, and timelines of information, thus supporting more efficient HR processes and procedures. Furthermore, it enables improvements for Manpower Modelling, Crisis Establishment (CE), and Crises Response Operations (CRO) by reducing analysis and reporting workloads and through the production of standardised executive summaries and reports. It also enables the usage of a single identity token for physical and logical access control, visual identification and entitlement tracking.

Service Features:

This service can be tailored by the customers selecting the required service features (applications and portals) only. Service features are grouped into service flavours as below:

- **Applications in scope of this Service - Service Flavours**

APP032-1 Flavour Personnel and Manpower Management System – APMS Application:

APMS is a highly configurable and modular software suite designed for military organisations consisting of four core areas: Post and Organizational management, Personnel Management, Manpower and Manning Reporting, and Billeting. APMS draws data from the full spectrum of existing sources, which is then exploited to provide Commanders and Staff with an aggregated, costed, synchronised and timely view of the full spectrum of military activity.

The flavour cost is calculated based on which of the following sub-flavours are required.

Sub Flavours:

- **APP032 – 1.1 APMS NATO Enterprise O&M** – including the centralized costs of the APMS NATO Enterprise APP032 instance O&M and support which are minimally required for the common funded organizations. (Mandatory for all common funded organizations covered by ACO CSLA: ACO, NISFR, ACT, IMS, NSO, STO CSO, STO OCS, NDC).

- APP032 – 1.2 APMS NATO Enterprise Access – including only the access to the APMS NATO Enterprise APP032 instance (mandatory for non-common funded organisation), includes remote support for non ACO CSLA organizations – except NAEW&CF.)
- APP032 – 1.3 APMS Mobility - includes an NCIA managed mobility device with access to the NATO Enterprise APMS instance.

Note:

This Flavour requires access to the NATO Enterprise Instance as a prerequisite; Alternatively, customer may purchase the APMS Mobility sub-flavour (charged per device) which includes an NCIA managed mobility device with access to the NATO Enterprise APMS instance.

APP032-2 Flavour Establishment Review – ERT Application:

ERT application allows to perform regular changes to establishments and organizational details (i.e. Establishment review (approx. every 5 years), Units reviews (approx. every 3 years), Crisis Establishments change every 6 months, Individual Post Changes (many each year).

The flavour cost is calculated based on which of the following sub-flavours are required.

Sub Flavours:

- APP032 – 2.1 ERT NATO Enterprise O&M – including the centralized costs of the ERT NATO Enterprise APP032 instance O&M and support which are minimally required for the common funded organizations. (Mandatory for all common funded organizations covered by ACO CSLA.
- APP032 – 2.2 ERT NATO Enterprise Access – including only the remote support and access to the ERT NATO Enterprise APP032 instance (mandatory for non-common funded organisation).

Note:

This Flavour requires APMS as a prerequisite;

APP032-3 Flavour Workflow Management System – Genpact Sequence Application:

Sequence application is a COTS component within APMS used to design, develop, maintain and execute HR business work-flows. Existing workflows: NSTEP processing, Out-processing, In-processing, Absence Management, Skills Self Certification.

The flavour cost is calculated based on which of the following sub-flavours are required.

Sub Flavours:

- APP032 – 3.1 Sequence NATO Enterprise O&M – including the centralized costs of the Sequence NATO Enterprise APP032 instance O&M and support which are minimally required for the common funded organizations. (Mandatory for all common funded organizations covered by ACO CSLA.

- APP032 – 3.2 Sequence NATO Enterprise Access – including only the remote support and access to the Sequence NATO Enterprise APP032 instance (mandatory for non-common funded organisation).

Note:

This Flavour requires APMS as a prerequisite;

APP032 - 4 Flavour Card Identification and Security Management – AMIS Application;

AMIS is the NATO card management system authorized to provide unique NATO ID card for physical access for NATO personnel as well as encoding user and administrator certificates onto PIV (Personal Identity Verification) smart card for computer system authentication.

The flavour cost is calculated based on which of the following sub-flavours are required.

Sub Flavours:

- APP032 – 4.1 AMIS NATO Enterprise O&M – including the centralized costs of the AMIS NATO Enterprise APP032 instance O&M and support which are minimally required for the common funded organizations. (Mandatory for all common funded organizations covered by ACO CSLA.
- APP032 – 4.2 AMIS NATO Enterprise Access – including only the remote support and access to the AMIS NATO Enterprise APP032 instance (mandatory for non-common funded organisation).
- APP032 – 4.3 AMIS Web Enrolment (optional) – including the configuration of customer's existing end-device for AMIS enrolment – requires connectivity to NATO Enterprise Instance, camera and signature pad and agreement with another entity for printing and shipping the AMIS cards (not included)
- APP032 – 4.4 AMIS Issuance Kiosk (optional) – including the license, configuration of customer's existing end-device for AMIS card issuance and support of the connected TOPPAN printer – requires connectivity to NATO Enterprise Instance, TOPPAN Printer, card stock and peripherals (not included)
- APP032 – 4.5 AMIS Mobility (optional) – including an NCIA managed mobility device (laptop), AMIS issuance license and its configuration – requires TOPPAN Printer, card stock and peripherals (not included)
- APP032 – 4.6 AMIS Card Printing (optional) – allows customer to outsource the printing of the AMIS badges – requires AMIS Web Enrolment and customer to pick up or take care of the shipment of the AMIS cards (location as agreed).

Note:

This Flavour requires APMS as a prerequisite;

APP032-5 Flavour Privileges and Immunities Management – NSTEP Application;

NSTEP is a tax-free privilege system allowing NATO AMIS ID card holders to receive, consume and track their privileges and entitlements offered by NATO host nations.

The flavour cost is calculated based on which of the following sub-flavours are required.

Sub Flavours:

- APP032 – 5.1 NSTEP NATO Enterprise O&M – including the centralized costs of the NSTEP NATO Enterprise APP032 instance O&M and support which are minimally required for the common funded organizations. (Mandatory for all common funded organizations covered by ACO CSLA.
- APP032 – 5.2 NSTEP NATO Enterprise Access – including only the remote support and access to the NSTEP NATO Enterprise APP032 instance (mandatory for non-common funded organisation).

Note:

This Flavour requires AMIS as a prerequisite;

APP032-6 Flavour Installation Access Control System – NIACS Application;

NATO Installation Access Control System provides the capability to verify the validity of a NATO AMIS ID card as well as checking the access to a given installation or security area.

The flavour cost is calculated based on which of the following sub-flavours are required.

Sub Flavours:

- APP032 – 6.1 NIACS NATO Enterprise O&M – including the centralized costs of the NIACS NATO Enterprise APP032 instance O&M and support which are minimally required for the common funded organizations. (Mandatory for all common funded organizations covered by ACO CSLA.
- APP032 – 6.2 NIACS NATO Enterprise Access – including only the remote support and access to the NIACS NATO Enterprise APP032 instance (mandatory for non-common funded organisation).

Note:

This Flavour requires AMIS as a prerequisite;

APP032-7 Flavour ISIPS: Installation Visitor Management and Host Nation Support;

ISIPS allows Registration Offices to record and manage host nation specific personnel information as well as register vehicles with local authorities. The system allows reporting on relevant information focusing on site and host nation regulations. ISIPS allows Security forces and International Military Police to record visitors, visitors passes, vehicle visitors and link them with the sponsor information allowing them to create meaningful reports for longer periods of time.

The flavour cost is calculated based on which of the following sub-flavours are required.

Sub Flavours:

- APP032 – 7.1 ISIPS NATO Enterprise O&M – including the centralized costs of the ISIPS NATO Enterprise APP032 instance O&M and support which are minimally required for the common funded organizations. (Mandatory for all common funded organizations covered by ACO CSLA.
- APP032 – 7.2 ISIPS NATO Enterprise Access – including only the remote support and access to the ISIPS NATO Enterprise APP032 instance (mandatory for non-common funded organisation).

Note:

This Flavour requires APMS as a prerequisite;

APP032-8 Flavour Performance Management System – NPMS Application;

Performance Management System allows HR community to perform the Annual Performance Appraisal for NATO International Civilians, setting annual objectives and performing the need it mid-term and annual reviews.

The flavour cost is calculated based on which of the following sub-flavours are required.

Sub Flavours:

- APP032 – 8.1 HR Portals NATO Enterprise O&M – including the centralized costs of the HR Portals NATO Enterprise APP032 instance O&M and support which are minimally required for the common funded organizations. (Mandatory for all common funded organizations covered by ACO CSLA.
- APP032 – 8.2 HR Portals NATO Enterprise Access – including only the remote support and access to the HR Portals NATO Enterprise APP032 instance (mandatory for non-common funded organisation).

Note:

This Flavour requires APMS as a prerequisite;

- **Activities in scope of this Service:**

Service Management of entire service lifecycle including regular user communication;

Supplier Management:

- Management of the required 3rd party contracts (contract signature, extension or termination as required)
- Monitor delivery of 3rd party services/goods;

Application Management:

- **New Capability Development:**

- Requirements Analysis, Solution proposal, Cost estimation, Development (including SW changes with 3rd party vendors as required) and Assignment of changes into logical release packages;

- **Incident Management:**
 - Issue Investigation and Resolution; Escalation of tickets to 3rd party supplier when required and follow up until their final resolution;
- **Independent Verification & Validation:**
 - Change Configuration Proposal (CCP) Submission and Follow up;
- **Deployment:**
 - Configuration & Reconfiguration;
 - Deploying & Release, and Patches Management;
- **Operations:**
 - Operate and perform the required maintenance on the application servers and the underlying platform.
 - Operate and perform the required maintenance on the databases including backup, restore and replication.
 - KPI Monitoring
 - Maintenance of the related AD Components;
 - Set up and Maintenance required Reference/Test and Development environment in DEVOPS and make it available for the Senior User representatives.
 - Sequence Management;

Service Flavours:

The APMS is a core Flavour, while AMIS, NIACS, NSTEP and ISIPS are extended flavours that can be added to meet specific customer needs.

Available on: NU, NS, and NPCL.

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)
 WPS002 Enterprise Identity Access Management Service
 WPS008 Enterprise Service Operations Centre Service
 SEC015 Security Certificate Service
 LEG008 Local Other Service

Underlying Services: PLT008, OTH001, SME005

Standard Service Support Levels:

Service Availability¹ Target: 99.5%

Service Restoration: for NCS customers, the restoration priority will be as specified in centralised or local service level agreement.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes



Service Cost / Price:

The cost is calculated **per Flavour per Number of Posts**. The price details available in the Service Rates document.

APP033 INTEL FS Application Service

Service ID: APP033

Service Name: INTEL FS Application Service

Portfolio Group: Application Services

Service Description: The Intel FS (Intelligence Functional Service) Application Service provides an integrated, robust and flexible capability supporting a suite of services available throughout the Bi-Strategic Command (Bi-SC) Automated Information System (AIS) to support the direction, collection, processing, and dissemination of intelligence in a timely and responsive manner in accordance with NATO policy, doctrine and guidance.

Value Proposition: Intel FS Application Service provides the NATO Intelligence Community with a capability that enables the following operational benefits:

- Sharing of intelligence services and data across NATO at all levels of command.
- Manage the direction, collection, processing, and dissemination of intelligence requirements.
- Enhance the dissemination of intelligence with Nations and other domains.
- Enhanced analysis and exploitation capabilities.
- Manage posting and publication of intelligence products.
- Information exchange supporting situational awareness, common operational picture and targeting.
- Support the management of the intelligence processes.
- Provide search and analytical capabilities to retrieve/analyse intelligence information.
- Support the generation and the management of Intelligence Information.
- Provide specialised functionalities in support of specific domains (imagery, local employee personnel, and battlespace objects).
- Provide intelligence collaboration and synchronisation mechanisms to share intelligence across NATO according to Communities of Interest.
- Support interoperability with external systems.
- Manage Users and Permissions.
- Support all operational mission types.

Service Features: The INTEL FS Application Service is comprised of the following features that combined support an overall intelligence cycle:

- Intelligence Direction (Request For Information (RFI) and Intelligence Requirement Management).
- Intelligence Search, and Analysis.
- Intelligence Processing – creation/management of intelligence products such as Battle Space Objects (BSO) and Intelligence Surveillance Reconnaissance products (ISR Products).
- Intelligence Management.
 - Maintenance of Intelligence products.

- Intelligence Dissemination.
 - Dissemination of intelligence products to the intended recipients.

Service Flavours: The INTEL FS Application Service can be fully customized and provided with different components enabled/disabled: LEP, RFI, Imagery, ASAS products, RSS, Administration, Domain Value management, CSD, etc.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side)
APP055 Core GIS Geospatial Service

Underlying Services: PLT008, OTH001, SME005

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9026	Intelligence Functional Service (INTEL-FS) Basic User
A9027	Intelligence Functional Service (INTEL-FS) Battle Space Objects (BSO)
A9032	Intelligence Functional Service (INTEL-FS) Organisational Node Administration (ONA)
A9044	NATO Intelligence Functional Areas Services Training (NIFST)
A9061	Intelligence Functional Service (INTEL-FS) Intelligence Request Management
A9064	Intelligence Functional Service (INTEL-FS) System Administrator

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP034 Integrated Engineering Management (IEMS) Application Service

Service ID: APP034

Service Name: Integrated Engineering Management (IEMS) Application Service

Portfolio Group: Application Services

Service Description: The Integrated Engineer Management System (IEMS) Application Service is an integrated asset management tool, which provides operation, support, maintenance and infrastructure management functionalities.

Value Proposition: The IEMS Application Service enables the user to support the maintenance of the SHAPE Infrastructure within accepted and agreed response times as per SHAPE' requirements. In addition, this application enables infrastructure project management, supports material management and SHAPE property disposal business processes.

Service Features: The IEMS Application Service offers a modular approach in support of the SHAPE Base Support Group within one single centralized database:

- Project Management
- Buildings Management
- Warehouse Management
- Budget Management
- Budget Long Range
- Reimbursable Customers Management
- Bunker Management
- Capital Items Management
- Non-expendable Items Management
- Utilities Consumption Management
- PWL Personnel Management
- Timekeeping Management
- Fire Brigade Management
- Proposal Disposal Office Management

Service Flavours: The IEMS Application Service is available as a single offering.

Available on:

NATO Unclassified

The Service may be available on other security domains upon a New Service Request.

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side)

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP035 eLeave Application Service

Service ID: APP035

Service Name: eLeave Application Service

Portfolio Group: Application Services

Service Description: The eLeave Application Service provides an organisation with an online environment, which allows it to effectively and easily manage and administer all Human Resources leave related activities in an automated and standardized manner.

Value Proposition: The eLeave application service provides a fully automated system, which supports the organization's HR leave processes. In doing so it delivers a standardized, accurate and paperless online environment in which employees, managers and Human Resources administrators can easily and efficiently manage leave activities; i.e. : "leave requests", "approval / rejection", "leave balances & statuses", ... As such it covers all the process steps; from leave submission to the eventual and final approval or rejection. The implementation of such a system greatly reduces the time and effort spent on the management and administration of all leave related activities and processes. Moreover, the e-leave IT system provides standardization across all HR leave activities. It should be noted, that it has been developed fully in line with NATO's HR processes, activities and business rules.

Service Features: The eLeave Application Service allows users, i.e. staff members, to request all types of leave (Annual Leave, Home Leave, Special Leave for Private Reasons, Special Leave on Marriage, Special Leave for Maternity and Paternity, Long Service Leave, Leave for Training, Leave for Military Service or Training and Unpaid Leave). The Service can also be used to report absence for health reasons (Sick Leave). In addition the service provides:

- Leave record for each staff member, including leave balances and home leave entitlements
- Automatic calculation of leave days (based on official holidays per duty location)
- Automatic e-mail notifications and tasks for approval
- Attachments (for sick leave certificates, etc.)
- Creation of calendar appointments from leave requests
- Personal detailed leave overviews for the staff members
- Reports for managers at various organizational levels
- Versioning of all leave data
- Archiving of previous years' requests
- Consideration of Annual leave cut-off dates in calculations
- Recording and parking of next year's leave to be processed by the end of the year

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side)

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period is 8 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Database.

APP036 Finance (FinS) Application Service

Service ID: APP036

Service Name: FinS Application Service

Portfolio Group: Application Services

Service Description: FinS provides the user with an Enterprise Resource Planning (ERP) system (based on the Oracle E-Business Suite Commercial Off-The-Shelf software and some extensions (iTravel)) with capabilities to perform streamlined budget execution, accounting, procurement, payments, and travel processes. It allows the customer to be compliant with NATO Financial Regulations (NFRs), Procurement Directives and International Public Sector Accounting Standards (IPSAS).

The FinS Application Service provides O&M support for existing FinS implementations.

Value proposition: FinS offers the user greater transparency, flexibility, control and auditability over allocated and delegated budgets, thus facilitating NATO Strategic Commands, NATO Military Commands, NATO Agencies and other NATO Organizations focusing on their core business.

Service Features: FinS provides the following functional features:

- General Ledger;
- Accounts Payable;
- Accounts Receivable;
- Cash Management;
- Fixed Assets;
- Purchasing;
- Advanced Procurement (iProcurement, Procurement Contacts, Service Procurement);
- Travel Management (Travel Requests and Travel Claims);

FinS consists out of the following elements:

- FinS Operations: Daily management of hardware and software;
- FinS Incident and Problem Management;
- FinS Change Management: Change management in coordination with concerned stakeholders;
- FinS Training.

Service Flavours: The service is available as a single flavour, with available specific configurations.

Available on:

NATO Unclassified
NATO Restricted

Service prerequisites:

This service provides O&M support only. An implementation project, possibly including the procurement of software licenses, is a prerequisite.

NDW001 NATO Digital Workplace Service (Low Side) / WPS006 REACH Mobile Workplace Service

Underlying Services: PLT008, OTH001

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP038 NATO Talent Acquisition Application Service

Service ID: APP038

Service Name: NATO Talent Acquisition Application Service

Portfolio Group: Application Services

Service Description: The NATO Talent Acquisition Application Service provides the customer with a modern, fully electronic capability to effectively and efficiently support recruitment campaign in line with NATO directives. This application supports the recruitment process from vacancy posting, video interviews, to successful candidate selection and onboarding for civilian personnel and various types of temporary workers at the NATO International Staff Centre, NATO International Military Staff, NCI Agency and NATO Alliance Ground Surveillance Management Agency.

Value Proposition: The NATO Talent Acquisition Application Service drives a significant reduction in cost for the execution of a recruitment campaign and seriously improves operational efficiency and quality results through the use of the application. This is achieved through increased automation of tasks as it accelerates the recruitment campaign. The application offers automated workflows and a single point to access the web-based front end for the applicants and the specialized application frontend and backend for the hiring managers and hiring officials. The use of the application enables effective, efficient, quality, faster and less-costly management of recruitment campaigns. Through its introduction, the application eliminated the need to print and distribute a large number of documents for the various stakeholders involved in the recruitment process. As the capability is built on one single database instance, but with built-in data segregation for each NATO entity, it allows each organization to remain in control of its own recruitment campaigns but also for the HR officials to share data and knowledge about candidate application history as needed. Additionally this service, through its search and apply functionalities, offers the applicant a greater recruitment experience.

Furthermore, this application increases NATO's image and branding as an employer through the presentation of vacancies to a larger number of NATO bodies onto the same online recruitment platform and in the improvement of results, through attracting a wider range of active and passive candidates.

Service Features: The NATO Talent Acquisition Application Service offers the user recruitment campaigns; online job-boards; collection and management of applications; asynchronous video interviews, recruitment screening and evaluation tools, together supporting candidate selection and store and share of application histories.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side)

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP039 P3SM and Workflow Application Service

Service ID: APP039

Service Name: P3SM and Workflow Application Service

Service Type: Supporting Service

Portfolio Group: Application Services

Service Status: Available

Service Description: The P3SM Application Service provides the user with Portfolio, Program, Project and Service Management capabilities to support the creation and execution of related processes and activities. The P3SM Application Service provides project start-up/planning/baselining/execution/control/collaboration, resource management, time accounting and reporting.

The Workflow Application Service provides the platform for all internal agency processes to be automated and digitised via web-based interfaces. The Workflow Application Service is responsible for automating and supporting a growing catalogue of core agency processes such as: Business Intake, Workforce Planning, Business Execution Planning and IIT Requirements Collection.

Value Proposition: The P3SM Application Service enables the enforcement of common project management procedures, data centralization and improved accuracy and control to project progress, expenses, resource management, execution & control and reporting. Furthermore, projects utilizing the P3SM Application Service benefit from easier redirection of resources to meet project demand and real-time monitoring of project performance.

The Workflow Application Service ensures internal agency processes are executed efficiently. The service removes manual process bottlenecks, reduces the burden of repetitive and time-consuming tasks from staff whilst also drastically improving data-quality and accurate process auditing and reporting.

Service Features:

- Project Execution and Control; Efficient execution of project controls towards effort and cost;
- Time Accounting System; allows project staff resources to report project/non-project activities and time spent;
- Project Collaboration; based upon SharePoint technology enables store/share/act on projected related information (documents, issues, risks).
- Automation of internal processes; Potential for any internal process, regardless of complexity, to be digitised.
- Workflow management; Allows process owners to administer and configure their own applications
- Data-Management; a bonus feature of the workflow platform is the ability to create web-based data-management tools
- Reporting; Configurable reporting functionality

Service Flavours: The Service is available in two flavours; The P3SM application flavour and the Workflow Application flavour.

Available on:

NATO Restricted

Service Prerequisites:

WPS006 REACH Mobile Workplace Service

PLT003 Web Hosting Service

PLT006 Database Platform Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A3000	PRINCE2 Foundation & Practitioner Certification Exam Preparation
A3001	MSP Practitioner Certification Exam Prep
A3002	Project Management Professional (PMP) Exam Prep
A3019	Microsoft Project Introduction
A3028	Project Management Training: Skills for Success
A3043	Agile Project Management Training for Practitioner & Foundation Certification

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP040 Enterprise Asset Management Application Service

Service ID: APP040

Service Name: Enterprise Asset Management Application Service

Portfolio Group: Application Services

Service Description: The Enterprise Asset Management Application Service provides an ERP system based on Oracle E-Business Suite Commercial Off-The-Shelf Software, the capabilities of which are to collect, process, present and distribute consolidated information of assets, from a lifecycle perspective (acquisition to disposal). This service supports the centralized management of assets and is technically integrated within the centralized NATO Automated Financial System (CNAFS Application Service) to drive better visibility on reporting, decision-making, sustainable financial discipline, regulatory compliance (Inventory IPSAS 12), data integrity, optimized and efficient asset management processes. The Service provides the capabilities for operating Logistics in compliance with the Property Accounting Directives ACE 60-80 and the NCIA 'Under Construction Successor for the superseded NCSA OSI A-16-04.

Value proposition: The Enterprise Asset Management Application Service offers centrally managed Inventory and Order Management capabilities, with delegation of specific operational tasks to the local CSU's, integrated with already existing procurement and finance capabilities to drive efficiencies in the lifecycle of asset management. Furthermore, amongst other benefits, utilizing the Inventory/Asset Management Application Service facilitates easier redirection of asset resources as well as improving the operating costs by avoiding duplicated procurement and rationalizing inventory and assets including traceability.

Service Features: The Enterprise Asset Management Application Service offers the following features:

- Inventory Management (Warehouse Configuration Management, Asset Receiving, Creation and Labelling, Stock Availability Planning); Item management, asset movement, physical inventory and periodical cycle counting, inventory replenishment, reporting, quantity and value management.
- Order Management; customer account / CisPOC(MRAH) Assignment / custodian / shipping / delivery addresses management, internal/external.
- Asset Cost Accounting; asset valuation/weighted average cost (WAC) calculation, inventory accounting/reconciliation and auditing.
- Approval Hierarchy along with automatic notifications defined in the system also ensures control and visibility of Asset Procurement and movements.
- Auditing capabilities inherently present in the system can be used to fulfil internal/external checks and also for KPI's for any performance improvements.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

NATO Restricted

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side)

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP041 Logistics Functional Area Services (LOGFAS) Application Service

Service ID: APP041

Service Name: Logistics Functional Area Services (LOGFAS) Application Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Available

Service Description: The LOGFAS Application Service enables the user to collect, store, manage, analyse, present and distribute information related to deployment and sustainment, logistics and host nation support for forces during NATO operational planning and execution.

Value Proposition: The standardization of logistics data and data formats and their timely exchange is the key to the success of complex logistics operations, especially to facilitate the coordination for deployment, reinforcement and sustainment of forces from multiple nations, with limited logistic assets and infrastructure. LOGFAS addresses the requirement to minimize the planning time for NATO deployments and to maximize the capability for rapid exchange of the associated plans, reports and other information to enable orderly flow of movements into, from and within theatre.

Service Features: The LOGFAS Application Service is comprised of multiple modules, these are:

- **LOGFAS Viewer** – LOGFAS Viewer provides the staff officer access to LOGFAS data via a web application. It presents situational awareness information on the force status and the infrastructure for the selected Plan or Operation in a format configured useable at the Strategic, Operational or Tactical level.
- **ADAMS/ADAMS Web** – Allied Deployment and Movement Systems module supports multinational deployment planning through provision of deployment plan development, feasibility estimation and Host Nation Support Concept of Requirements.
- **EVE/EVE Web** – Effective Visible Execution provides monitoring of movement and transportation activities and provision for plan adjustments during execution. EVE Web enables movement visibility and transport request management.
- **CORSOM** – Coalition Reception, Staging and Onward Movement provides visualization and oversight of theatre movements, during both deployment, execution and sustainment operations.
- **SPM/SDM** – Sustainment Planning Module provides calculation functionality to support sustainment requirements for operations.
- **GEOMAN** – Provides geographical information on the facilities, unit holdings and transportation networks. GEOMAN is also used to manage the Host Nation Support Capability Catalogue (HNS CAPCAT).
- **LDM** – This module enables maintenance, reporting and import/export of information on force profiles and holdings, supplies, packaging, consumption rates, transportation assets, and planning data.

- **LOGNET** – LOGNET is the collaboration portal for the logistics community operating on both NATO Unclassified and NATO Secret platforms.

Service Ordering and Request: *[describes the procedure, which is required for customers to request the service or product; describes the means by which customers can report incidents and problems related to the use of the service or product – **usually equal for all services**, unless an exceptional procedure is required → this attribute will not be shown in the Catalogue, unless being exception from the standard for all services]*

Service Flavours:

The service is available in multiple flavours:

APP041-1	LOGFAS Product Lifecycle Support Services
APP041-2	LOGFAS Instance
APP041-3A	LOGFAS User Support Small
APP041-3B	LOGFAS User Support Medium
APP041-3C	LOGFAS User Support Large
APP041-4	LOGFAS New Instance
APP041-5	LOGNET Instance

The detailed description of the service flavours are provided in the Annex below.

Available on:

- Any network of customer
- NATO Secret
- Mission Secret, VeVA
- NATO Unclassified (LOGNET)

Service Prerequisites: Infrastructure compatible with the requirements of the application as described in the release documentation.

Standard Service Support Levels:

Service Availability¹ Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting: Periodic reporting as agreed with the customer.

Available NCI Academy Training not covered by service cost:

0222	LOGFAS Operational Movement Planning Course (CORSOM)
0223	LOGFAS Movement Execution and Coordination Course (EVE)
0224	LOGFAS Strategic Deployment and Movement Planning Course (ADAMS)
0225	LOGFAS Strategic Deployment and Movement Planning Advanced Course (ADAMS)
0251	LOGFAS Staff Officer Course

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

0252	LOGFAS Movement and Coordination Advanced Course (EVE Advanced)
0253	LOGFAS Sustainment Planning and Distribution Course (SPM/SDM)
0254	LOGFAS Fundamentals and Data Operator Course
0255	LOGFAS System Administrator

Service Cost / Price: The cost of service is composed of a product life cycle support cost which is a necessary cost to keep the product running regardless of the number of sites running the application, the product lifecycle support unit of measure is unit 1. There is also a cost for deployment and support flavours depending on the size of the site, the unit of measure for these flavours is per site. The cost details are listed in the service rate section of this catalogue release.

Annex – APP041 Service Flavours Detailed Descriptions

LOGFAS Product Lifecycle Support services (APP041-1)

This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of the specified application. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year.

The cost drivers for product lifecycle support include:

- **Service Portfolio Management**
- **Segment Architect**
- **Product Change Management Governance**
- **Service Delivery Management** – This service is responsible for the day-to-day operations of the logistics functional services and ensures the smooth delivery of IT services to customers and end-users. Service delivery focus is on the operations, quality, and improvement of services throughout their lifecycle within agreed levels of service.
- **Application Maintenance** – This service is subject to Change Management Governance by Change Control Board (CCB), led by SHAPE J6/J4. Typically, one major release and two minor releases are planned each year. All new versions are backward compatible.
- **License Management**
- **Release Management** – This service includes the efforts to package, build, test and release the new LOGFAS Versions. LOGFAS Releases undergo various testing processes to ensure that the product is interoperable, fit for purpose and use, and ready to be made available. These activities are performed by various NCI Agency teams as well as user communities, ranging from functional SMEs to security experts.
- **Exercise Planning Support**
- **Reference Data Management** – As the designated Reference Data Manager by SHAPE for Reportable Item Codes (RIC), Transportation assets and Host Nation Support Facilities, this effort covers the configuration management and release of new versions of data sets in the reference data areas.

LOGFAS Instance (APP041-2)

This flavour provides for a single running copy (instance) of LOGFAS on specified network domain with its own specific setup, configuration and user access. This includes the maintenance and support for the running instance, such as OS upgrades and application upgrades, hot-fixes, and backup and recovery management. This flavour does not include underlying costs of hosting infrastructure and platform of the instance. The cost drivers include:

- **Enterprise Change Management Governance**

- **1st Level Support** – This service is provided by local Command Support Units. They are the initial point of contact for technical issues, and disruptions.
- **2nd Level Support** – This service is provided by C2BA Centralised Level 2 Support. It includes fixing configuration issues, troubleshooting, deployment of upgrades and hot-fixes.
- **3rd Level Support** – This service is provided by C2BA and contractors. It provides the highest level of specialist skills available in order to fulfil support requests.

LOGFAS User Support (APP041-3)

This flavour offers user access management and user support for all levels of users. The flavour applies to one site for a defined number of users with applicable sizes listed in Table 1. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year. The cost drivers include:

- **1st Level Support** – This service is provided by local Command Support Units. They are the initial point of contact for user inquiries, technical issues, and disruptions.
- **2nd Level Support** – This service is provided by C2BA Centralised Level 2 Support. It includes fixing configuration issues, troubleshooting, and access management. This service is provided via an operational level agreement with the C2BA Centralised Level 2 Support team and costed as such.
- **3rd Level Support** – This service is provided by C2BA and contractors. It provides the highest level of specialist skills available in order to fulfil support requests.
- **On-site Support visits** – This service is provided by C2BA and contractors. It provides a limited number of short on-site support visits to provide the highest level of specialist skills available in order to fulfil support requests on-site.

User Support sizes	Number of users	On-site support visits
APP041-3A User Support Small	Up to 25	None
APP041-3B User Support Medium	Between 25 and 100	1x5 days with 2 people
APP041-3C User Support Large	Above 100	1x5 days with 2 people 1x5 days with 6 people

LOGFAS New Instance (APP041-4)

This flavour offers implementation of a new instance on any supported security domain. The cost includes: the feasibility study, one requirement workshop at customer premises, installation and configuration and initial knowledge transfer.

LOGNET Instance (APP041-5)

LOGNET is the collaboration portal for the logistics community operating on both NATO Unclassified and classified platforms. NCI Agency provides content management, storage and access control services.

This flavour provides for a single running copy (instance) of an application on specified network domain with its own specific setup, configuration and user access. This includes the

maintenance and support for the running instance, such as OS upgrades and application upgrades, hot-fixes, and backup and recovery management. This flavour does not include underlying costs of hosting infrastructure and platform of the instance. The cost drivers include:

- **Enterprise Change Management Governance**
- **2nd Level Support** – This service is provided by C2BA Centralised Level 2 Support. It includes fixing configuration issues and troubleshooting.
- **3rd Level Support** – This service is provided by C2BA and contractors. It provides the highest level of specialist skills available in order to fulfil support requests.

APP043 Interactive Simulation Package (ISP) Application Service

Service ID: APP043

Service Name: Interactive Simulation Package (ISP) Application Service

Portfolio Group: Application Services

Service Description: The service provides a flexible, state-of-the-art solution to support the execution of air operations, which enables nations to simulate radar data in order to generate plot data to use it in a training and/or testing environment.

Value proposition: The service enables conduct of testing and exercises by providing necessary radar data.

Service Features: ISP enables generation of necessary data for execution of exercises for air operations, with particular focus at the NATO Integrated Air and Missile Defence System (NATINAMDS) community. More specifically, it enables:

- Modelling of airborne, sensor, and ECM exercise elements and to engineer scenarios by retrieval, positioning, manoeuvring, altering and manipulation of various elements via the graphical user interface;
- Performing of scenario management (retrieve, save, add, build, merge and delete);
- Performing of preview functions on the scenario;
- Execution and control of scenarios by starting, stopping, pausing, rewinding and forwarding the exercises;
- Activation and deactivation of radar sensors;
- Performing of interactive “real-time” changes, upon request, to alter the scenario during scenario execution;
- Providing of exercise support for flight plan printouts of selected missions and providing of the generation of flight plans, visible within the Multi AEGIS Site Emulator (MASE) system or any other system using the ADEXP flight plan message format for direct flight plan injection;
- Providing of realistic training for operational crews in the use of mechanical and electronic counter-measures (chaff simulation);
- Allow for the control of simulated fighter aircrafts using manoeuvrable targets

ISP is a standalone product, supported on Solaris, with the NISP configuration for the Solaris installation as preferred one. ISP provides input to the MASE system, but does not dependent on the MASE baseline version.

Service Flavours:

NCS-wide ISP software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, and documentation of maintenance releases of all ISP software components and the continuous support of the eligible user sites.

Available on:

NATO Secret

NATO Classified

Service prerequisites:

PLT013 (former APP051) NATO Integrated Secure Platform (NISP)

Standard Service Support Levels:**Support Hours:**

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)

Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number:

Belgium +32 65 44 3177

Netherlands +31 70 374 3177

Italy +39 081 721 3177

Germany +49 282 4978 3177

USA +1 757 747 3177

For NATO HQ +32 02 707 5858

Service Requests:

To request the APP043 service please complete the Customer Request Form and contact NCI Agency Demand Management.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

Due to the nature of the ISP service (standalone, client-only software application, used for training simulation purposes often on unreachable non-production / non-NATO networks) no service availability monitoring KPIs are defined.

In case an SLA is established for ISP support the standard NCI Agency service support KPIs (response and restoration times) apply unless otherwise negotiated.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions between NCIA and SHAPE on an annual basis.



APP045 SIGINT COINS Application Service

The Service is classified. Further information is available upon request and relevant clearance.

APP046 HMART Application Service

Service ID: APP046

Service Name: HMART Application Service

Portfolio Group: Application Services

Service Description: The Human Intelligence (HUMINT) and Counter Intelligence (CI) support service offers subject matter expertise (SME) support to the applications used by HUMINT and CI. The applications facilitate users to collect intelligence provided by human sources. It includes the systematic and controlled collection and exploitation of HUMINT/CI by interaction with human sources, objects, or individuals. HUMINT and CI activities involve safeguarding and exploitation of human sources, and efficient collection, reporting and analysis integrated within the overall intelligence environment to provide decision makers with timely and accurate information necessary for conducting successful military operations.

Value proposition: HMART consists of two separate but related modules that address the HUMINT requirements (HMART SD and HMART OM). The modules combined provide support to the HUMINT process for NATO lead operations ranging from:

- Securely managing the highly sensitive identities of human sources,
- Support to HUMINT mission planning.
- NATO HUMINT doctrine standards based report writing (AIntP-5).
- Workflow driven life cycles of reports providing the mechanism to improve the quality of reporting and ensure the proper sanitization of information.

HMART OM also embeds a module LEP (Locally Employed Personnel) that support the CI Vetting processes within operational theatres.

Service Features: HMART consists of three modules that serve different parts of HUMINT and CI operations.

HMART SD (Source management and de-confliction) – a stand-alone module running on secured and ruggedized laptops within NATO lead operations. The purpose of the module is to maintain information that could potentially reveal the identity of the source. The module has the following functionalities:

- Management of a dossiers of human sources
- De-confliction of human sources based on biographic and biometric characteristics.
 - Biometric comparison based on biometric modalities of face and finger print information.
 - Biographic (or heuristic) characteristics that are the basis for de-confliction other than biometrics. Eye colour, estimated year of birth, living location, weight, tribe and many other fields considered to identify possible duplicate sources.
- Secured exchange of source information within the J2X command structure.
- Powerful search functions to allow for analytical processing of source information. Structured searches based on metadata fields, geographically oriented search and unstructured full text search in order to quickly identify the human source coverage within an area of operation.

HMART OM (Online Module) – an online reporting module for HUMINT operations and support to HUMINT mission planning.

- Internal and external report writing based on NATO HUMINT doctrine (AIntP-5)
 - Fragmentation Order (FRAGO)
 - Debriefing Area Reconnaissance (DBA RECCE)
 - Contact Form
 - HUMINT Report
 - CI Report (CI)
 - Liaison Contact Report (CI)
- A workflow driven report life cycle that contributes to timely reporting and improved quality of reports produced.
- An operations (OPS) matrix used for HUMINT mission de-confliction at J2X level.
- Support to analytical processes. E.g. identify the operational value of a source based on information provided by a source.
- Interoperability with J2 for external reports (CI Report and HUMINT Report)
- A central repository for all HUMINT reporting containing historical reference data and supports data analysis.

LEP – an online module to support the Locally Employed Personnel vetting procedures.

- Management of a dossiers of LEP's, Screening files, addresses, employment etcetera.
- De-confliction of LEP's based on biographic and biometric characteristics.
 - Biometric comparison based on biometric modalities of face and finger print information.
 - Biographic characteristics that are the basis for de-confliction other than biometrics. Eye colour, estimated year of birth, living location, weight, tribe and many other fields considered to identify possible duplicate sources.

Sub-Services:

- HMART implementation, integration and customization.
- Operations and maintenance (HW and SW upgrade, annual biometric maintenance licences, release and change management, system administration, monitoring, etc.).
- Training of HMART users and administrators either at the NCI Agency, HUMINT Centre of Excellence (HCOE) or on-site.
- HMART support during the preparation and conduct of operations, exercises and experiments.
- Information gathering for technical and training support.

This service provides full or partial technical and training support in the HUMINT information gathering, process and design, and production of tailor made reports.

Service Flavours: HMART supports HUMINT/CI operations by two distinct operational modules.

HMART SD – deployed on stand-alone laptops to provide the best protection of the identities of human sources.

HMART OM – as a networked capability used within the J2X structure for reporting and support to HUMINT/CI mission planning.

LEP – as a networked capability used within the J2X structure for vetting locally employed personnel. Can be integrated within HMART OM.

Available on:

NATO Unclassified (Training and exercise only)
NATO Secret (HMART OM/LEP)
NATO Secret stand-alone (HMART SD)

Service prerequisites:

HMART SD

HMART SD is designed to run on stand-alone ruggedized laptops (TEMPEST level B) with hardware encrypted HDD when used for operational purposes.

HMART OM/LEP

HMART is a fully web based application that requires a server installation. Client machines only require a HTML5 compatible browser like Chrome, IE11 or MS Edge.

Underlying Services: OTH001, PLT008

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9015	J2X Intelligence Systems

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP047 Open-Source Intelligence (OSINT) Service

Service ID: APP047

Service Name: Open-Source Intelligence (OSINT) Service

Portfolio Group: Application Services

Service Description: : The OSINT service provides to the Open Source Intelligence (OSINT) analyst and NATO Open Source researchers a complete toolkit to collect, process and exploit online data through a managed attribution platform, consume commercial OSINT services with the Janes Defence Foundation and Current intelligence datasets, and access online subscriptions on NS through the ACO Open Source System (AOSS) platform.

Value Proposition: An estimated 80% of required information available for use in open sources for specific information vital for a deep analysis is available in newspapers, magazines, industry newsletters, television transcripts, and blogs. . Furthermore, an industry of curated intelligence collection has emerged on which the NATO OSINT analysts increasingly rely. By using OSINT services, the Intel Analysts are able to get pertinent and essential information in the most effective way.

The use of OSINT has grown within the private sector as well as being a mainstay of the military and the intelligence services for years.

Service Features:

Key features of the service are proper managed attribution, access to Janes Defense commercial database of Battle Space Objects (BSO) for correlation and a complementary web based application giving users easy access to data from licenses and open source data on the NATO classified networks.

Service Flavours:

The OSINT/OSINT service comes in 3 distinct but complementary components.

- [new] Managed attribution service: the managed attribution service allows the Open Source Researcher to access the Internet from the NATO UNCLASSIFIED network through a commercial platform providing a layer of customization of its digital identity. There is a limited number of licenses for the Managed Attribution service currently.
- [new] Janes Defense commercial database service: the Janes Intara service allows the Open Source Researcher to access the Janes Foundation and Current intelligence datasets, directly from the Janes' unclassified online portal, or later in 2026 through an API on the ITM network. The Janes Defense Service is only available to NATO Enterprise users.
- AOSS service: a centralized web-based application that constantly collects open and subscribed source information from news agencies and Internet and transfers it in real time to the different networks within NATO. The web based application facilitates other functions to support the OSINT analysts to prepare their intelligence reports.

Available on:

Online commercial Software as a Service
NATO Unclassified



NATO Secret
Mission Secret (on demand)

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: PLT008, OTH001, SME005

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardized SLA.

Available NCI Academy Training not covered by service cost:

A9039	Allied Command Europe Open Source System (AOSS)
A9044	NATO Intelligence Functional Areas Services Training (NIFST)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP048 Analyst Notebook (ANB) Application Service

Service ID: APP048

Service Name: Analyst Notebook (ANB) Application Service

Portfolio Group: Application Services

Service Description: ANB offers a visual analysis environment designed to help analysts to turn large sets of disparate information into high-quality actionable intelligence and to help identify, predict, and prevent criminal, terrorist, and fraudulent activities. A flexible data acquisition approach allows analysts to more quickly collate both structured and unstructured information to help build a single, cohesive intelligence picture. The flexible data model and visualization environment coupled with a wide range of visual analysis tools help users build multiple views for detailed network, temporal, statistical, or geospatial analysis and reduce the time taken to identify key connections, networks, patterns and trends that may exist. The results gained from this detailed analysis may be shared via intuitive and visual briefing charts or visualizations that can be included in end intelligence products.

Value Proposition:

- Flexible data acquisition: rapidly import structured data, simplify the manual data entry process, connect to and query available data sources.
- Flexible data model and representation (environment that offers users flexibility in how data is modelled and visualized).
- Simple communication of complex data (intuitive and easy-to-follow visual briefing charts).
- Powerful analysis capabilities (wide range of analysis capabilities).
- Extensibility (see *Service Flavours*).

Service Features: The Analyst Notebook (ANB) Service offers the user:

- Acquire data from disparate sources in order to piece together a coordinated picture that allows for an effective, more accurate analysis of available information.
- Establish key “who, what, where, when and why” information by analysing and visualizing data in multiple ways including association, temporal, geospatial, statistical, spreadsheet views and social network analysis, “list most connected” and “find connected networks”.
- Identify connections, patterns, trends and key intelligence within a wide range of data types that might otherwise be missed.
- Discover duplicate information within data by leveraging intelligent semantic smart matching capabilities.
- Increase understanding of structure, hierarchy, method of operations and key individuals or groups within criminal, fraudulent and terrorist networks and the roles they may play, helping to guide future operational planning and resource allocation.
- Create clear and concise briefing charts to simplify complex data in support of more timely and accurate operational decision making.
- Simplify the communication of complex data to enable timely and accurate operational decision making.

- Capitalize on rapid deployment that delivers productivity gains quickly using a well-established visual analysis solution.

Service Flavours: The service is available as a single flavour. However, there is an extensive range of options available to extend further i2 Analyst's Notebook capabilities in order to provide even greater value to analysts and their wider organization. These come with additional costs:

- **Data Centric Analysis**—IBM i2 Analyst's Notebook Premium
- **Data Acquisition**—IBM i2 iBridge, IBM i2 Information Exchange for Analysis Search
- **Geospatial Analysis**—IBM i2 Analyst's Notebook Connector for ESRI
- **Unstructured Data Analysis**—IBM i2 Text Chart, IBM i2 Text Chart Auto Mark
- **Collaboration**—IBM i2 Analyze (via i2 Analyst's Notebook Premium), IBM i2 iBase
- **Extensibility**—IBM i2 Analyst's Notebook SDK

Available on:

NATO Unclassified
NATO Secret
Mission Secret (MS)

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: OTH001, SME005

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9014	NATO Use of IBM Analyst-s Notebook User

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP049 Integrated Command and Control (ICC) Application Service

Service ID: APP049

Service Name: Integrated Command and Control (ICC) Application Service

Portfolio Group: Application Service

Service Description: The NATO-wide Integrated Command and Control Software for Air Operations (ICC) is an integrated Command, Control, Communications and Intelligence/Information (C3I2) system that provides information management and decision support to NATO air operation activities during peacetime, exercise and crises. Currently, ICC provides functional support for the most critical Air C2 functions at the Joint Force Command, Air Command, and Combined Air Operations Centre levels as well as limited BMD functions. ICC consists of client and server applications, which can also be operated by different organisational elements. An organisational element can opt to utilize only ICC clients as standalone workstations (e.g. for parsing ATOs) or when allowed to connect to another element's ICC server for planning data and/or to a NIRIS server for RAP data.

Value Proposition: ICC provides capabilities for integrated planning, tasking, operations, information management and decision support to operational and tactical level air operations during peacetime, exercise, crisis and conflict. ICC also supports critical Air Command and Control (Air C2) functions at Air Component Command (ACC/JFACC) and Combined Air Operations Centre (CAOC) levels.

Service Features:

- Generation of Air Operations Directives (AOD)
- Generation of Airspace Control Orders (ACO)
- Generation of Air Tasking Orders (ATO)
- A capability for executing current operations at ACC/JFAC and CAOC units
- Automated status reporting
- Display of a Joint Common Operational Picture (COP) including the Recognized Air Picture (RAP) as provided from the Networked Interoperable (near) Real-time Information Services (NIRIS)
- Display of Shared Early Warning (SEW) information.
- TMD situational awareness and missile engagement (LSID)
- Replication of ICC related C2 data between sites
- Web-services interface to provide Air C2 information to interfacing systems

Service Flavours:

NCS-wide ICC software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and deployment of maintenance releases of all ICC software components and the continuous support of ICC sites throughout the NATO Command Structure (NCS).

ICC client: Provides the ICC Client application on NDW002 NATO Digital Workplace Service (High Side) including local configuration to connect to (remote) ICC servers and other NATO FAS, version updates and continuous support.

ICC server: Provides an ICC Server on INF004 provided server infrastructure, including local configuration, version updates and continuous support.

Available on:

NATO Secret
Mission Secret

Note: APP049 is not provided on national security domains as the NCI Agency can only support as a service and guarantee service levels for ICC instances that reside on NATO networks. Nations can get ICC support for their national security domains via the SME007 service Bundle D.

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side). ICC clients require this service, which provides a standard NATO workstation connected to the NATO networks on which the ICC Client application can be deployed.

INF004 - Infrastructure Virtualization Services to provide the server instance (either physical or virtual) on which the ICC Server components can be deployed.

PLT013 (former APP051) NATO Integrated Secure Platform (NISP) Service. The ICC server service flavour requires the NISP service as NISP is the recommended platform for ICC server on NATO networks.

Oracle - The ICC Server support service requires a licenced Oracle database instance for ICC.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177

For NATO HQ +32 02 707 5858

Service Requests:

To request the APP049 service please complete the Customer Request Form and contact NCI Agency Demand Management.

https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall ICC availability will be measured as an aggregate of all the individual availabilities of the components listed below.

ICC functional component	Service Level Target (availability)	Performance threshold (determining when service is considered unavailable)
Airspace Management (ASMAN) (ACO generation)	99.5%	CRUD operations response < 5" for up to 25 concurrent users
Air Operations planning (SALTO) (ATO generation)	99.5%	CRUD operations response < 5" for up to 50 concurrent users
Mission (ATO) execution monitoring (MTOTE, OB TOTE, CADAP)	99.5%	CRUD operations response < 5" for up to 150 concurrent users
RAP Display	99.5%	delay < 15" for up to 5,000 tracks
COP Display (Map)	99.5%	Responsive to map interaction (TBD)
BMD Situational Awareness (LSID, SEW)	99.5%	TBD
ICC DB replication (ICC Link)	99.5%	Heartbeat
ADATP3 message interface (MIMI) (ACCS-ICC interface)	99.5%	Heartbeat

KPIs implementation: ICC already contains some internal monitoring functionality. The necessary changes to expose the above availability KPIs are planned for implementation as part of the product roadmap.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1000	Combined NISP ICC System Administrator (CNIC)
A1001	Windows ICC System Administrator (WICC)

A9009	Integrated Command and Control (ICC) Data Manager
A9010	Integrated Command and Control (ICC) User

Service Cost / Price: Unit of measure used for service quantification for each flavour can be found in the table below:

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP049	Integrated Command and Control (ICC) Application Service	NCS-wide ICC software maintenance and in service support	1
APP049	Integrated Command and Control (ICC) Application Service	ICC client	Per client
APP049	Integrated Command and Control (ICC) Application Service	ICC server	Per server

APP050 Air Command and Control Systems (ACCS) Application Service

Service ID: APP050

Service Name: Air Command and Control Systems (ACCS) Application Service

Portfolio Group: Application Services

Service Description: Air Command and Control System (ACCS) provides Air Command and Control (AirC2) and Ballistic Missile Defence (BMD) services through a modern and integrated system being deployed at various user sites. It enables seamless Air C2 and BMD operations across multiple ACCS locations.

The Air Command and Control System (ACCS) First Level of Operational Capability (LOC1) is deployed to operational units at the NATO Command Structure (NCS) and the NATO Force Structure (NFS) contributing to SACEUR's NATO Integrated Air and Missile Defence System (NATINAMDS). ACCS is comprised of a core software providing the main functionality, site adaptation and is installed and operated dedicated hardware and COTS software platform. The ACCS core software is configurable to build ACCS entity types which realise a specific operational capability at various levels of command. This includes the Combined Air Operations Centre (CAOC), Air Control Centre/RAP Production Centre/Sensor Fusion Post (ARS), the BMDOC build on TMD1 functionality and in the future, after implementation for the Addendum 3 System Adaptation, the Joint Force Air Command. A CAOC or an ARS entity may be static or deployable and a combined implementation of a CAOC and an ARS constitutes a CARS (Combined ARS).

Value Proposition: The value of ACCS is the integration of almost all relevant functions and external interfaces required for executing seamless Air C2 and (T)BMD Operations within a network of ACCS sites at different level of command. Those functions can be installed at static sites as well as implemented as deployable or mobile site configurations.

Service Features:

The ACCS LOC1 covers the following Air C2 related operational functions:

- C2 Resource management including configuration planning, tasking and monitoring;
- Air Space Management including planning and utilization of the air space and mission preparation;
- Surveillance including Air Picture Production and related asset management;
- Air Mission Control including Air Policing Management, aircraft and SAM control;
- Force Management including allocation planning and tasking (A/C and SAM units);
- Air Traffic control including integration with civilian Air Traffic Control (ATC) centres and sensors.

ACCS TMD1 augments above ACCS operational functions to build (tactical) Ballistic Missile Defence (BMD) specific functionality utilized as the main system at the Ballistic Missile Defence Operations Centre (BMDOC). This (T)BMD specific functionality build by ACCS TMD1 covers Surveillance Operations, Sensor Management, Planning and Tasking,

Engagement Operations, creation, visualization of a (T)BMD picture and dissemination to BMD sites.

Service Flavours: ACCS consists of several standardized entity types which are used in different combinations to build ACCS operational sites at different level of operational command.

As prerequisite for these flavours, centralised ACCS Core software maintenance is being executed and NCS wide In-Service-Support is provided to ACCS sites within the NCS. The ACCS Core software maintenance delivers site specific ACCS baseline and security updates is a pre-requisite for below service flavours offered to operational units:

OPS Level	Services
(D)ARS	The (deployable) ARS is a combination of the individual ACCS entities ACC, RPC and SFP. The Air Control Centre (ACC) executes air mission control within a dedicated area of operational responsibility (AOR): • Covers real-time (RT) battle management; • Performs air mission control for all types of manned air missions and SAM weapons; • Provides ATC services. The RAP Production Centre (RPC) enables air surveillance by producing and disseminating the Recognised Air Picture (RAP) data within its assigned AOR: • Receives land and maritime surface tracks and sub-surface tracks from external links and disseminates them to the ACCS users. • Manages its subordinate and allocated ACCS surveillance areas in accordance with orders and priorities received from the CAOC. The Sensor Fusion Post (SFP) contributes to air-surveillance by receiving data from various sensor sources and building a local air picture as basis for establishment and the maintenance of an RAP at the RPC: • Develops a local air picture (LAP) through the fusion of data from both active and passive sensors; • Reports on the status and performance of subordinate sensors; • Controls the sensor detection and responds to anti-radiation missile (ARM) threat and electronic counter-measures (ECM) activity.
(D)CAOC	The (deployable) CAOC is the entity in charge of the tasking of the assigned air assets, it:

	- Plans and conducts the tasking of air operations and C2 resources configuration within a designed AOR; - Supervises and monitors execution of tasking and analyses the results; - Coordinates with land, maritime and national forces as well as with other NATO and National agencies.
TMD1	ACCS TMD1 represents an entity specifically configured to provide the main C2 service for the BMD Operations Centre (BMDOC). It enables specific (T)BMD functions comprising: - Surveillance Operations, - Sensor Management, - Planning and Tasking, - Engagement Operations - Creation, visualization of a (T)BMD picture and - Dissemination of the (T)BMD specific picture BMD related sites.
ACCS Deployable Assets	ACCS deployable elements augments ACCS operational entities like and ARS or CAOC to become deployable or mobile. It comprises: - Deployable/Transportable Equipment; - Deployable active and passive Sensors; - Interfacing Equipment & CIS Security Boundary Protection; - Communication Equipment and - Deployment support packages and primary mission support equipment.

Available on:

NATO Secret

Service Prerequisites: ACCS requires a dedicated operating platform consisting of CIS hardware, communications, COTS Software ACCS functional software and ACCS operational data. Data exchange with external system and between ACCS sites requires to be protected through firewalls as well as security appliances realised by Application Layer Firewall or Boundary Protection Devices:

SEC022 – Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service

- Mandatory for interfacing with:
 - Military and civilian sensors for receiving sensor data,
 - Military sensors for sensor control,
 - Civilian ATC centres for receiving ATC flight plans.

INF028 – ACCS Sensor Integration Module (ASIM) Service

- Optional for converting military and civilian legacy sensor data formats into an ACCS conform sensor data format.

APP054 - L16@29k Application Service

- Optional for utilizing the L16@29K system to exchange Link 16 (Platform D) data with other platforms on the same Link 16 network.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)

Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident-problem / Service Request reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177

Netherlands +31 70 374 3177

Italy +39 081 721 3177

Germany +49 282 4978 3177

USA +1 757 747 3177

For NATO HQ +32 02 707 5858

To request the APP050 service please complete the Customer Request Form and contact NCI Agency Demand Management.

https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

Service Flavour	Service Level Target (availability)
All ACCS entity types (ARS, COAC, TMD1)	99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Technical hotline can be activated through the CSD and would within 2 hrs, provide technical remote assistance 24/7.

Available NCI Academy Training not covered by service cost:

A1002	ACCS System Manager
A1003	ACCS Security Officer
A1004	ACCS Communication Manager
A1008	ACCS-ICC interface Administration
A1016	ACCS Data Manager

Service Cost / Price: The unit of measure for the Service is 1 for all service flavours. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP050	Air Command and Control Systems (ACCS) Application Service	NCS wide ACCS software baseline maintenance and In Service Support (ISS) for NCS sites	1
APP050	Air Command and Control Systems (ACCS) Application Service	(D)ARS	1
APP050	Air Command and Control Systems (ACCS) Application Service	(D)CAOC	1
APP050	Air Command and Control Systems (ACCS) Application Service	TMD1	1
APP050	Air Command and Control Systems (ACCS) Application Service	ACCS Deployable Assets	1

APP052 Air Situation Data Exchange (ASDE) Gateway Service

Service ID: APP052

Service Name: Air Situation Data Exchange (ASDE) Gateway

[Currently implemented by the NCIA's Application Layer Firewall for Link 1 (ALFL1) product]

Portfolio Group: Application Services

Service Description: The purpose of the Air Situation Data Exchange Gateway service is to:

- Provide an operationally available and security approved Application Layer Firewall for Link 1 that can:
 - Act as a Boundary Protection Device that provides Boundary Protection Services (BPS) in accordance with the self-protecting node principle to provide protection of the infrastructure and to mitigate risk introduced by interconnecting networks working with different security classifications, e.g. to protect the Link 1 interface of NATO CRC's from external Link 1 connections
 - Deliver Information Protection Services (IPS) to enforce the information release policies, preventing unauthorized and uncontrolled release of information, ensuring that only the information intended to be exchanged are effectively transmitted under a controlled, security monitored regime, e.g. to allow the controlled exchange of unclassified Link 1 data with partner nations.
- Provide release and deployment services (installation), by leading or supporting all activities required for properly fielding of baselines to existing or new sites. This includes, but are not limited to:
 - Site survey and collection of site-specific installation information
 - In-house installation, configuration and system testing
 - Shipping and asset management services
 - On-site installation, configuration and operational testing
 - On-site training for ASDE Site Manager and ASDE Site Technician(s).
- Provide in-Service Support, by offering continues support to sites using Application Layer Firewall for Link 1 that includes:
 - First, Second and Third Level Support
 - On-site maintenance
 - Site Support
- Provide Security Services, in order to maintain agreed security posture. This includes:
 - Continuous liaising with security authorities to monitor updates in relevant security policies and directives and to implement any changes required.

- To implement new security patches from underpinning systems, perform regression testing, and make updates and installation procedures available to all registered sites by releasing Technical Bulletins at the AirC2 Systems' support sites on Internet (NU) and NSWAN (NS).

Value proposition: The Air Situation Data Exchange Gateway Service ensures that the Application Layer Firewall for Link 1 can act as a boundary protection device for NATO Link 1 connections, and realize NATO requirements for a bi-directional exchange of a RAP between NATO and Partner Nations. The Multi-Level Security system manages the controlled and monitored exchange of air picture data between networks of different information security and management policies.

Service Features: When exchanging data the system can operate in two states:

- 1) Filtering State, when exchanging Air Situation Data between an AirC2 system on HIGH classification (NS or NC) and a system with LOW classification (NR or NU).
- 2) Symmetrical State, when exchanging Air Situation Data between two systems on NC or NS.

Filtering State: Allows the exchange of the Air Situation with a Partner Nation by sanitizing the Link 1 messages to a level of NATO Unclassified. The filtering state offers four distinct modes:

- Peacetime Operations Mode
- Exercise Operations Mode
- Crisis Response Operations Mode
- Article 5 Operations Mode

The operational modes will determine the set of filter rules the Application Layer Firewall for Link 1 will apply and includes a pre-defined set of functionality by implementing:

- Coordinate conversion: masking of the originator site positions by using an arbitrary, bi-laterally agreed Data Link Reference Point (DLRP);
- Geographic filtering: selection of information for data exchange based on geographical areas;
- Data/Message filtering: message and data field filtering for sensitive information;
- Validation: message frame validation (on receipt from PN only).
- The Application Layer Firewall for Link 1 security enforcing capability provides the following capability;
- Trusted computing base: verification of message fields filtering and message frame validation.

Symmetrical State: The symmetrical state operates interconnecting two entities operating on NC and NS classification levels. As the RAP is classified NC only, the dissemination between those two entities does not require data filtering but only frame validation, in order to ensure that only Link 1 messages are exchanged.

Supported configuration and Interface Standards:

The Application Layer Firewall for Link 1 supports both filtering mode and symmetrical mode. Regardless of the mode, the software and hardware requirements are identical

and no change of hardware / software is required to alter the mode of operation. The mode of operation is in fact a configuration parameter to be controlled by the system administrator. The Application Layer Firewall for Link 1 implements the Tactical Data Link protocol Link 1 in accordance with STANAG 5501, edition 7.

The services currently installed is Application Layer Firewall for Link 1 version 4.0.1 and 5.0.0. These are NATO Baselines under the governance and Configuration Control of the AirC2 SC.

Service Flavours:

NCS-wide ALF-L1 product maintenance and in-service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and deployment of maintenance releases of all ALF-L1 system components and the continuous support of the eligible ALF-L1 sites both in NATO and PN's.

ASDE Gateway National Instance: For national use of ALF-L1 to provide Air Situation Data Exchange, an eligible Potential ASDE Partner (PAP) Nation should submit a written request to participate in ASDE programme to the NATO Air and Missile Defence Committee. According to the NATO Policy on ASDE PO(2017)0452 the Vice Chairman is then responsible to staff the request for approval by the relevant Alliance bodies and the NAC. After approval, a Customer Request Form may be submitted following normal procedures.

Available on: The Application Layer Firewall for Link 1 (NATO Side) supports any security classification as required by the data handled reaching from NC to NS. The ALF-L1 (Partner Side) supports any security classification as required by the data handled reaching from NU to NC. The product software itself is classified as NR and the system is delivered as an NR system with software pre-installed.

Service prerequisites:

- PLT013 (former APP051) NATO Integrated Secure Platform – (NISP) Service
- Existing serial Link 1 connections must be available
- Communication lines, network infrastructure

Standard Service Support:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)

Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request the APP052 service please complete the Customer Request Form and contact NCI Agency Demand Management.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

To find the latest updates and most recent information about this service, please visit:

Internet: <https://www.asc.nato.int> (password protected – please request account at amdc2.productservices@ncia.nato.int)

NS WAN: <https://airc2-iss.ncia.nato.int/support/>

KPIs:

Due to the nature of the ASDE service (software running at system-high mode on unreachable and non-NATO networks) no service availability monitoring KPIs can be defined.

In terms of service support metrics, the standard Agency KPIs (per priority response times) apply for remote support. In case local intervention is required, the restoration time will depend on travel options at the time of the incident.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: Unit of measure used for service quantification for each flavour is listed in the table below.

Service ID	Service Name	Service Flavour/Option	Service Unit
APP052	Situation Data Exchange (ASDE) Gateway	NCS-wide ALFL1 software maintenance and in service support	1

Service ID	Service Name	Service Flavour/Option	Service Unit
APP052	Situation Data Exchange (ASDE) Gateway	ASDE Gateway National Instance	Per instance

APP053 Multi Airborne Early Warning Ground Integration Segment Site Emulator (MASE) Application Service

Service ID: APP053

Service Name: Multi Airborne Early Warning Ground Integration Segment (AEGIS) Site Emulator (MASE) Application Service

Portfolio Group: Application Services

Service Description: The MASE Application Service provides a NCI Agency product and support of it, with the following purpose:

- Production of a real-time recognized air picture (RAP);
- Identification and exchange of the RAP with other military or civilian entities;
- Battlespace management and provision of weapons guidance solutions;
- Flight Plan processing and real-time interface to feeds supplied by ATC centres.

Value Proposition: MASE is a flexible, state-of-the-art solution to support the execution of air operations. Both military and civilian radars can be connected using a large variety of interface protocols on dedicated lines or packet switched networks. The sensor data from these sources is processed using a multi radar tracker, which produces the real-time air picture which can then be forwarded to other military installations. Flight plan data from civilian or military Air Traffic Control (ATC) centres are received, correlated with the real-time air picture and displayed to the operational user to support identification of aircraft. The Battlespace Management function assists the operational users in threat assessment and allocation of weapon resources. With the optional addition of the CRC System Interface (CSI), command and control can be performed on datalinks including Link 11(A&B) and Link 16. Threats can be engaged with either fighters or surface-to-air missile (SAM) units. When engaging with fighters, the assigned intercept controller can select between various types of guidance solutions depending on the fighters' capabilities and the prevailing tactical situation.

Service Features:

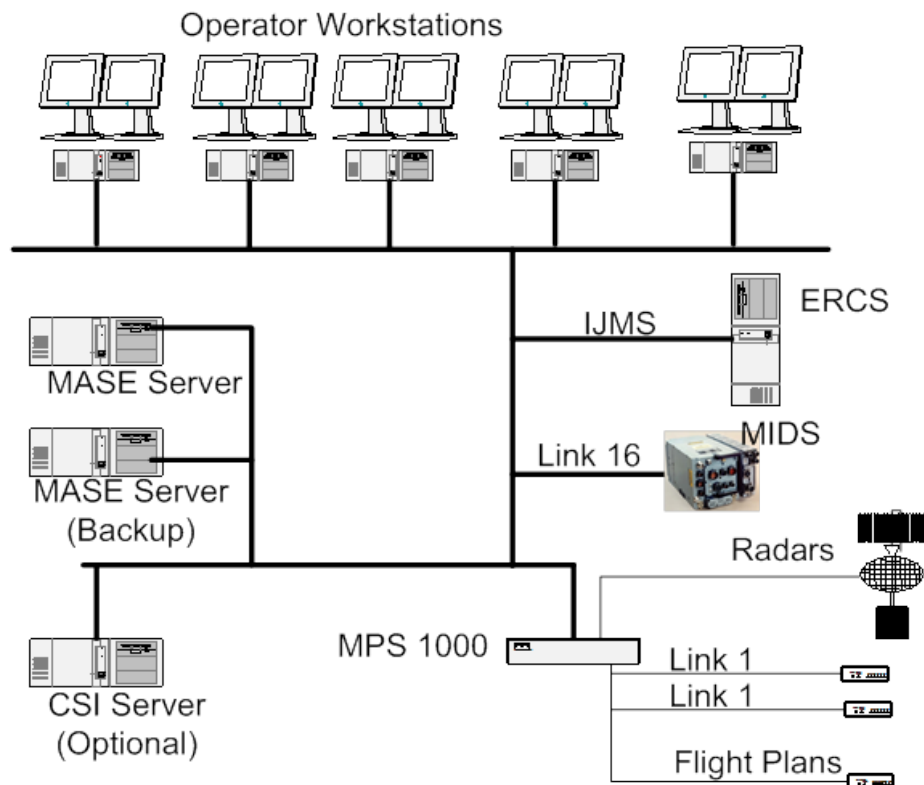
Sensor Integration – Allows to connect any number of radars to produce a locally generated Air Picture. Radar interfaces include but are not limited to : ASTERIX, JASR8, RMP, DDL, HADR, CD2, RSRP, T101, Cardion, T92, (A)S29, S743D, SRT, RAT31DL. The RAP produced is correlated into the Common Operating Picture (COP) and forwarded to connected units using the Link 1 interface.

Command and Control – Though the flight plan interface, tracks created from the RAP Production can automatically be identified. The Identification is managed with neighboring CRC's using the standard Link 1 messages for maintaining consistency across different military locations. The Weapons Allocator functionality allows for interceptor guidance and pairing to be performed. In addition, with the CRC System Interface (CSI) extension, Command and Control can be performed across the Link 11A/B and Link 16 datalinks. Enabling the operator to manage not only fighters but also land and naval units.

User Interface – The MASE User Interface has been completely re-designed, implemented upon a modern GUI engine and made more maintainable through the use

of Java development. In the future, the legacy console will be completely replaced by the new MASE Integrated Console Environment (MICE). MICE has been developed together with the NPC CSI Section to ensure that future HMI updates can be achieved in a quicker, more cost effective manner.

Below figure outlines MASE in a typical use case:



Supported configuration – MASE encompasses client server architecture, with dedicated server applications for the main tasks as real-time air picture establishment and interfacing external systems, interconnecting dedicated MASE operator workstations for the operational display through a standard UDP/IP network. The serial interfaces (for both radars and flight plans) are brought into the MASE system through the MPS-1000 serial interface device.

Supported Interface Standards – JASR8, RMP, DDL, (A)S29, RAT31DL, HADR, ASTERIX, CD2, RSRP, S743D, T101, Cardion, T92, SRT. Through the CSI, the following interface standards are supported: Link 16 Link 11A, Link 11B, ATDL-1, Link 22, FFI, VMF, OTHT-Gold.

Supported data link interfaces – Link 1 in accordance with STANAG 5501, IJMS .

Hardware- Software and CIS requirements:

- NCI Agency (NPC) Integrated Solaris platform (NISP) as a secured Solaris OS platform;

- X86 or SPARC based server HW able to run NISP/Solaris;
- MPS-1000 Serial interface server;
- Communication lines, network infrastructure.

MASE is supported by:

- Provision of MASE Software
- Helpdesk and provision of level 1 to 3 support through the Helpdesk
- On-site interventions for installation and/or trouble shooting
- Engineering/application support covering:
 - Product and Configuration Management;
 - Product baseline updates;
 - Safety assessment supporting a customer side SIL 1 claim.

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

PLT013 (former APP051) NATO Integrated Secure Platform (NISP) Service. The MASE server service flavour requires the NISP service as NISP is the recommended platform for MASE server on NATO networks. MASE clients can run on Windows environments and hence are not dependent upon PLT030.

Additional requirements:

- Existing serial Link 1 connections must be available
- Existing radar interfaces must be available
- If required, flight plan interfaces should also be available.

Service Flavours:

MASE software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and release of the MASE baseline to all sites registered for MASE. However, the sites themselves are responsible for the system update.

MASE instance installation and in service support: Upon request from non-NCS customers, MASE instances can be provided through an installation service. Such services and related support are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

Available on: MASE supports any security classification from NC to NS.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request the APP053 service please complete the Customer Request Form and contact NCI Agency Demand Management.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall MASE availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

MASE functional component	Target Availability	Performance threshold (initial access time)	Remarks
MASE Server Application (MSA)	≥ 99.5%	30"	Administrators should be able to load the MASE Server Application (AMA) within 30 sec.
MASE Console Application (MCA)	≥ 99.5%	20"	User should be able to access MASE Console Application (MCA) within 30 sec.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1011	MASE - MICE CONSOLE MIGRATION (MMC)

Service Cost / Price: Unit of measure used for service quantification for each flavour is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP053	MASE Application Service	MASE software maintenance and in service support	1
APP053	MASE Application Service	MASE instance installation and in service support	1

APP054 L16@29k Application Service

Service ID: APP054

Service Name: L16@29k Application Service

Portfolio Group: Application Service

Service Description: The Link 16@29K system allows a Host system to connect to a MIDS terminal and it:

- Allows the exchange of Link 16 (Platform D) data with other units on the same Link 16 network.
- Allows the MIDS terminal to be remotely controlled (On / Off Standby);
- Monitors the system discretes of the Link 16 Ground Equipment Suite.

Value Proposition: L16@29K allows the exchange of encrypted Link 16 data with other units on the same Link 16 RF Network. When connected through IP based crypto's the L16@29K allows for remote MIDS to be connected to a central C2 system

Service Features: L16@29K supports the following features:

- Local Mode : The L16@29K system is directly connected to the C2 host system using a MIDS Platform D interface. The MIDS is connected directly to an antenna at the physical location of the C2 host system.
- Remote Mode : The L16@29K system is situated in a remote location (due to UHF Coverage limitations). The system shares a platform D interface with the host system across an encrypted TCP IP connection. The MIDS is connected directly to an antenna at the remote location and is controlled remotely from the C2 host system.

Supported Interface Standards: The L16@29K system implements the Tactical Data Link protocol Link 16 in accordance with STANAG 5516, edition 2. The Platform D interface is currently supporting Block Cycle release 2. During 2021 the L16@29K Service will be updated to also include the Block Upgrade-2 (BU-2) interface for MIDS terminals.

Service Flavours:

L16@29K software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and release of the L16@29K baseline to all sites registered for L16@29K. However, the sites themselves are responsible for the system update.

L16@29K instance installation and in service support: Upon request, L16@29K instances can be provided to non-NCS customers through an installation and support service. Such services are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

Available on:

NATO Secret

Service Prerequisites:

None

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
 Netherlands +31 70 374 3177
 Italy +39 081 721 3177
 Germany +49 282 4978 3177
 USA +1 757 747 3177
 For NATO HQ +32 02 707 5858

Service Requests:

To request the APP054 service please complete the Customer Request Form and contact NCI Agency Demand Management.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall L16@29K availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

L16@29K functional component	Target Availability	Performance threshold (initial access time)	Remarks
L16@29K Application (LSA)	≥ 99.5%	10"	ACCS System capable of connecting to L16@29K Equipment Suite
MIDS Terminal Availability	≥ 99.5%	10"	MIDS Terminal capable of responding to interrogations from L16@29K Equipment Suite

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: Unit of measure used for service quantification for each flavour is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP054	L16@29K Application Service	NCS-wide L16@29K software maintenance and in service support	1
APP054	L16@29K Application Service	L16@29K Instance installation and in service support	1

APP055 Core Geographic Information System (GIS) Application Service

Service ID: APP055

Service Name: Core Geographic Information System (GIS) Application Service

Portfolio Group: Application Services

Service Description: The Core Geographic Information System (GIS) Application Service is composed of subservices, which serve multiple purposes. The service is primarily based on the commercial off-the shelf ESRI software provides other Functional Services with a common set of geospatial information (Geospatial Service) to ensure that 'everyone is operating off the same map', thereby eliminating the need for other FSs to develop their own mapping solutions and maintaining their own set of geospatial information. In addition, the Core GIS enables anyone in the NATO Command Structure (NCS) to see available geospatial information like maps or imagery. Core GIS provides base maps/foundation Geospatial Information (GI)/geo location reference to all users and systems. The Core GIS also contains a functional area system (Geography Service) for dedicated geo professionals to enable the Core GIS Geospatial Services to be managed and administered. The Geography Services is implemented at each NCS site with high-end workstations and displays, large format plotting, and scanning infrastructure.

Value Proposition: The Core GIS Application Service provides customers with a suite of data, services and products that ensure all phases of military operations are conducted on the same spatial reference. Furthermore, it provides the Accredited/Single Geospatial Information Service Provision (authoritative repository for Geospatial Information).

Service Features: The current Core GIS Application Service consists of:

Cartographic Workshop, which allows Geo-Technicians to create and maintain the Digital Geographic Information baselines, generate products, and publish and maintain geospatial services via the NATO Core GIS Server. The Cartographic Workshop comprises several high-end workstations for geo processing, and other peripherals such as an A0 plotter, A0 scanner, office printer, DVD production station, and infrastructure equipment

The Core GIS Server, which is used to provide geographic products such as electronic maps or other geospatial information in digital form to Functional Services and FASs using international standards such as Web Map Service (WMS), Web Feature Service (WFS), Web Coverage Service (WCS), Web Processing Services (WP).

Service Flavours: The service is available as a single flavour.

Available on: NATO Bi-SC Core GIS service is available on the NS, MS, KFOR and RSM network. However, the service may be available on the customer's choice of security domain, as well. In case of national security domain, the customer is responsible for the accreditation and license module.

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

Client: Windows 7 or Higher

Server: Windows 2012 R2 or Higher.

Detailed HW/SW requirements available upon request

Underlying Services: PLT008, OTH001, SME005, TRA002

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0300	Geo Basics Level 1
A0301	Geo Basics Level 2
A0302	Geo Scenario
A0310	Core GIS Servers
A9042	Combined Situational Awareness Functional Area Services for CTE/exercise

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP056 ISR Collection Management Tool (ICMT) Application Service

Service ID: APP056

Service Name: ISR Collection Management Tool (ICMT)

Portfolio Group: Application Services

Service Description: The ICMT Service provides a capability to effectively manage the satisfaction of Prioritized Intelligence Requirements (PIRs): plan, task, monitor theatre-wide ISR collection capabilities, manage intelligence documents, and disseminate products. It also facilitates the collection of short-notice requests and requirements in a timely manner. The ICMT Tool has two functions: Intelligence Requirements Management function (IRM) and Collection Management function (CM), of which IRM usually is not used by the NATO entities. Collection Management function supports users in developing and disseminating CRs. The purpose of CRs is to combine (or bundle) similar Essential Elements of Information (EEIs) from the ICP (similar with regards to locations, time and required ISR capabilities) to propose doing as much as possible with the limited ISR resources. CRs are recorded and tracked in the ISR Plan with associations to the EEIs that they satisfy in the ICP. The system provides support to process Collection Requirements List (CRL) and Collection Task List (CTL). When collection coordination is required CRs are passed up the chain of command as validated and prioritised CRs in the CRL. At the joint level CRs assigned to subordinate commands/units are disseminated as CTL. ICMT provides support to develop and disseminate Collection & Exploitation Plan (CXP). The CXP is the plan that provides detail of the tasks assigned to specific ISR capabilities to meet the formation's collection requirements. The CXP is based upon own formation's or CRs assigned from the JCMB received through the CTL. ICMT also provides functionality to disseminate CRs as ISR Requests and Tasks (ISRRs), and to manage received ISRRs.

Value Proposition: ICMT is a client/server solution making it possible for the different roles involved in the IRM & CM processes to work in parallel on a common database. Support for development of Intelligence Requirements and Intelligence Collection Plan (ICP) is provided in the new Intel Collection Plan workspace. Support for the management of Requests for Information (RFI) is improved and now supported in the new Requests workspace. Additional values are:

- Support for dissemination of the ICP in xml format.
- Support for development of both Collection Requirements (CR) and ISR Plans are new capabilities provided in the ISR Plan workspace.
- New capabilities to manage ISR Requests (ISRREQ) and ISR Tasks, which is a significant improvement of support for Collection Management. Collection Requirements can easily be exchanged between commands and ISR units as ISR Requests and ISR Tasks.
- Dissemination of the Collection Task List (CTL) in xml format is supported.
- Support to import of and export to excel sheets that comply with MAJIIC 2 Bravo .1 Baseline for the information content.

- Configurable to connect to the MAJIC 2 Bravo .1 JISR COI Technical Services enabling interoperability with national and NATO systems that are Bravo.1 compliant.

Service Features:

- Intelligence Requirement Management
 - Develop, receive, manage and track Priority Intelligence Requirements (PIRs) and IRs.
 - Developing and maintaining the ICP.
- Collection Management
 - Develop and disseminate CRs (CRLs and CTLs)
 - Process Collection Requirements List (CRL)
 - Process Collection Task List (CTL)
 - Develop and disseminate Collection & Exploitation Plan (CXP)
 - Functionality to disseminate CRs as ISR Requests and ISR Tasks (ISRRs)
 - Manage received ISRRs.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: PLT008, OTH001, SME005

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9030	Intelligence Collection Management Tool (ICMT)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP057 INTEL FS SIGINT Capability (ISC) Application Service

The Service is classified. Further information is available upon request and relevant clearance.

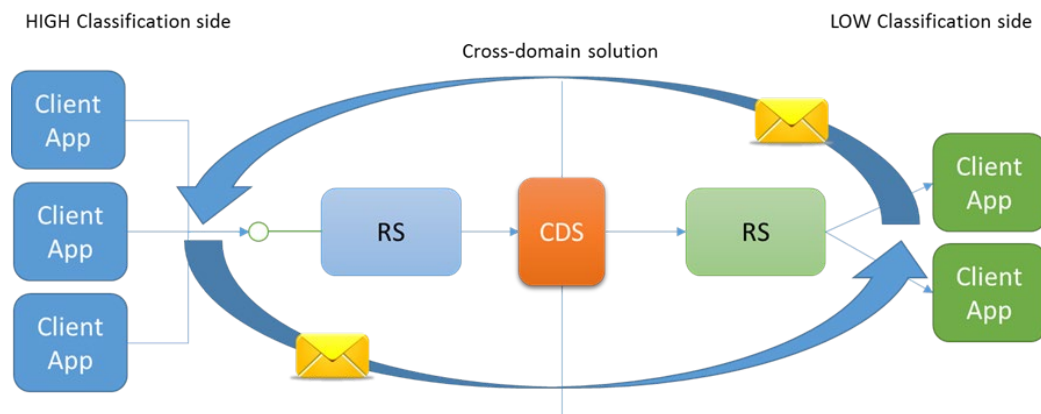
APP058 Release Server (RS) Application Service

Service ID: APP058

Service Name: Release Server (RS) Application Service

Portfolio Group: Application Services

Service Description: The Release Server (RS) service interface provides an abstraction layer for applications to release information between two security domains of different security levels. The service hides the complexity of Cross Domain Solutions for client applications.



Value proposition: The RS provides a service interface for applications to release information between two security domains of different security levels. The complexity of cross domain solutions are hidden behind a simple service interface. The Release Server supports automated and controlled release of information (a man in the loop scenario).

Service Features:

The Application features:

- Configurable release rules based on release-ability markings (Authority, Classification and Release-ability);
- Automated or controlled (man in the loop) release of information;
- Monitoring;
- Fully Web based user interface;
- Fully documented;
- Automated installation package.

Support features:

- * Support to implementation, integration and customization;
- * Support to operations and maintenance;
- * Support to training requirements;
- * Information gathering for technical and training support.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

Hardware:

- 64-bit architecture processor (multiple cores).
- Minimum 4 GB RAM (recommended 8 or 16 GB for operational use).
- 100 GB System drive.
- 500 GB Data drive minimum (depending on usage).

Software:

- MS Windows 2012 or newer
- IIS
- .NET Framework 4.6.2
- MS SQL Server 2008R2 or newer

The service can be configured remotely using a HTML5 compatible browser.

Underlying Services: PLT008, OTH001

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP059 Joint Exercise Development and Management (JEMM) Application Service

Service ID: APP059

Service Name: Joint Exercise and Management (JEMM) Application Service

Portfolio Group: Application Services

Service Description: The Joint Exercise Development and Management Application Service supports exercise training audiences in developing training objectives in a phased manner using a set of reference training objectives. JEMM subsequently supports exercise scenario designers in developing the MEL/MIL (Master Event List/Master Incident List) for an exercise in a structured and deliberate manner according to the process specified in the Bi-SC Directive 75-3. The application service also supports an exercise control organisation in executing the MEL/MIL during an exercise in a collaborative, distributed and interoperable manner. The exercise observation and analysis process is also supported. A specific flavour of JEMM supports the BMD community in executing BMD exercises by providing a direct interface to the BMD version of APP069 ITC.

Value Proposition: This application service supports exercise training audiences, exercise scenario managers, control staff, observers and analysts in performing their tasks in the preparation and execution of an exercise in a distributed and collaborative manner. It adds value to the process of developing, executing, observing and analysing an exercise by:

- Providing support for maintaining an organisational level of reference Main Capability Areas and subordinated tasks
- Providing support for a simple and advanced mode for developing training objectives. The advanced mode provides a controlled workflow for training audiences and training organisations to develop training objective descriptions to manage exercise resourcing conditions and achievability status and to set their priorities.
- Providing support for a collaborative and distributed way of working during the preparation and the execution of an exercise MEL/MIL.
- Providing a structured way of describing the MEL/MIL according to the Bi-SC 75-3.
- Establishing an explicit relationship between training objectives and MEL/MIL.
- Establishing explicit relationships between training objectives, observations and analysis
- Implementing a tailored workflow for the development and execution of a MEL/MIL.
- Implementing a tailored set of states for observations and analysis that are linked to training objectives.
- Providing, in a single configurable view, the elements of exercise information that are critical to the implementation of specific roles in the exercise control organisation.
- Providing the ability to add new sources of exercise information without having to modify the exercise control business applications.

- Documented capability to rapidly build exercise control dashboards using regular office automation tools.
- Providing the ability to configure and manage the execution of automated real time or periodic reporting data feeds capable of depicting ground, air, maritime, logistic and intelligence pictures.

Service Features: The JEMM Application Service supports the distributed, collaborative and structured development, execution, observation and analysis of an exercise MEL/MIL. Specifically, JEMM offers the following features:

- Prepare and develop the MEL/MIL as specified in the Bi-SC 75-3 Directive.
- Prepare and describe the synchronisation with simulation-based or live support to the exercise.
- Manage the execution of the MEL/MIL
- Manage the synchronisation of activities with simulation-based or live support to the exercise.
- Prepare and manage the collection of observations by observer/trainers.
- Analyse the collected observations and assess the progress of training objective achievement.
- Assign roles and rights to various users to perform tasks relevant to their participation in the exercise.
- Tailor the workflow of the execution and observation processes.
- Document MEL/MIL, observations and analysis results.

In addition the JEMM Application Service provides a structured, documented distributed access to configure data access to other NATO-operated exercise services like JTLS, JCATS and VBS as well as the ability to user-provided data in Excel spreadsheets. Access to specific JOCWATCH incident data is also supported. In order to visualize and exploit the combined data in an effective manner, JEMM offers a number of features that enables an exercise control organisation:

- To compose and visualize an exercise common operational picture in a distributed and collaborative manner.
- To de-conflict MEL/MIL with training audience activities and battle rhythm meetings
- To gather and extend MEL/MIL dashboards.

The JEMM Application Service also includes the feature to generate a subset of AdAt-P3, and OTH-GOLD messages as well as tactical links according to Link 16 and NFFI standards from data provided by the NATO-operated exercise services JTLS, JCATS and VBS.

In a specific BMD mode, the JEMM application service can be configured to communicate with the ITC (BMD) simulation service provided by APP069. Through JEMM, ITC simulation actions can be executed at scheduled times and the simulation state can be returned and processed by the automated reporting features to deliver an effective near-real time BMD recognized picture.

Service Flavours: The service is available as two flavours. A non-BMD and a BMD flavour.



Available on:

NATO Secret
Mission Secret
PAN

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: OTH001

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A5002	MEL/MIL
A5004	JEMM Data Administrator
A5006	Joint Exercise Management Module (JEMM) system administrator

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP060 - ISR Coalition Shared Data (CSD) & Imagery Intelligence (IMINT) Service

Service Name: ISR Coalition Shared Data (CSD) & Imagery Intelligence (IMINT) Service

Portfolio Group: Application Services

Service Description: The Service provides a comprehensive data, workflow, and application framework to support coalition Intelligence, Surveillance, and Reconnaissance (ISR) operations. This includes:

- **Data Capabilities:** The procurement, release, and integration of commercial imagery data and services (such as analytics), as well as the ingestion and management of multi-source ISR data (e.g., Full Motion Video, GMTI, MSI/HSI, LIDAR and Electronic Interceptions).
- **Workflow Support:** Enabling the full ISR Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) cycle across multiple echelons, services, and nations—facilitating the coordinated flow of data and intelligence products.
- **Applications:** Customer-facing applications relying on Coalition Shared Data (CSD) including exploitation tools (such as imagery), IRM&CM applications, and Sensor Systems. Currently supported applications include HMART, ICMT, INTEL-FS, and various national applications.

This integrated approach empowers coalition partners to store, discover, access, and share heterogeneous ISR libraries, ensuring timely and efficient exploitation of ISR resources in support of mission objectives.

Key capabilities include:

- Enables the exchange of NATO Intelligence, Surveillance and Reconnaissance (ISR) products through provision of a standard interface for storing, discovering, accessing and sharing heterogeneous ISR libraries maintained by NATO and Nations;
- Provides workflow support to the overall JISR Process of Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) spanning multiple echelons, multiple military services and multiple NATO and national applications and services; and
- Provides access to live or recorded Streaming Data types, such as Full Motion Video, Video Clips, or Ground Moving Target Indicator (GMTI) data
- Enables dynamic procurement of imagery and derivative intelligence products from commercial providers (e.g. satellite imagery, analytics), its normalization, cross-domain upstream transfer, and integration in the classified imagery server for exploitation.
- Enables the planning, data-management, human and machine-assisted exploitation, and structured observation management (SOM) of imagery, for Electro Optical (EO), Infra-Red (IR), Synthetic Aperture RADAR (SAR), Multi and Hyper Spectral (MSI and HSI), Light Detection and Ranging (LIDAR), Ground/Maritime Moving Target Indication (GMTI/MMTI) and Full Motion Video (FMV).

Value Proposition: The Service supports the JISR systems, workflows, and processes in order to provide the right (intelligence) information, at the right time, in the right format and to the right location for commanders to make the right decisions.

Service Features: The Coalition Intelligence, Surveillance, and Reconnaissance (ISR) Framework provide capabilities across the following categories:

- [new] Imagery exploitation suite: planning, data management, automated pipelines, exploitation client and SOM creation.
- [new] Commercial imagery service acquisition: vendors' management, dynamic tasking, bidding process, contracting and data management.
- CSD ISR Product Library: storage, discovery, access and dissemination.
- CSD ISR Workflow: support for JISR Collection Management and TCPED.
- CSD ISR Streaming: access to live or recorded streaming data types.

Supported JISR data formats, interfaces, and technical service contracts: STANAG 4545, STANAG 4609, STANAG 4607, STANAG 5516, STANAG 4559, and MAJIC2 Bravo .1 Baseline.

Service Delivery Models: The Service is offered in various configurations, depending on the combination of the following independent component services:

- ISR Product Library Services.
- ISR Workflow Services.
- ISR Streaming Services.
- [new] Commercial imagery and derivative products acquisition.
- [new] Imagery Intelligence Exploitation service.

Available on:

- NATO Secret
- Mission Secret
- NATO Unclassified

Service Prerequisites:

- NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)

Underlying Services:

- PLT008
- OTH001
- SME005

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP061 Air Command and Control Information Services (AirC2IS)

Service ID: APP061

Service Name: Air Command and Control Information Service (AirC2IS)

Portfolio Group: Application Services

Service Description: The Air Command and Control Information Service (AirC2IS) is the Air Functional Service including Ballistic Missile Defence (BMD) of the Bi-Strategic Command Automated Information System (Bi-SC AIS) for all levels of the NATO Command Structure. It is a non-real-time Command and Control service, which provides the NATO air staff with an integrated, robust, flexible and automated capability to effectively plan, execute, monitor and assess Air Operations (including BMD operations) in a responsive and timely manner. Together AirC2IS and the Air Command and Control System (ACCS) provide NATO's complete Air C2 capability. AirC2IS is an integrated suite of applications that addresses the Air Command & Control (AirC2) requirements at the operational and strategic level, as specified in the Allied Joint Publication (AJP) 3.3(A). AirC2IS supports the NATO AirC2 cycle.

Value proposition: AirC2IS evolves with the collaboration of the operational community for the operational community to provide an integrated, robust, flexible and automated capability to effectively plan, execute, monitor and assess Air Operations in a timely manner. It is designed with a focus on collaboration and multi-system integration. It ideally supports the operational level planning, assessment and information knowledge management processes. It is especially suited to the joint environment at static or deployed locations.

Service Features: AirC2IS acts as an information hub between the air mission area and other mission areas (land, maritime, special operations forces, intelligence, logistics, and others). To be able to do this, AirC2IS consumes information from and provides services to several NATO systems, including ICC, NIRIS, LOGFAS, and NCOP.

Following functionalities are included in AirC2IS:

Mission Applications:

- Interactive Map
- C2OA Manager
- ORBAT Applications
 - Generic Catalogue
 - Own ORBAT Manager
 - OPFOR ORBAT Manager
 - Neutral ORBAT Manager
- TBMD Applications
 - OPFOR TBM COA Manager
 - PCAL Manager
 - JPCAL Manager
 - IDDM
 - SAWREP Manager

- Tactical Information Display
- CONOPS Manager
- Support to Air Logistics
- AOD Editor

Information Portal:

- HQ Portal
- Mission Portal

Service Flavours:

NCS-wide AirC2IS software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and deployment of maintenance releases of all AirC2IS software components and the continuous support of the eligible AirC2IS sites throughout the NATO Command Structure (NCS).

AirC2IS server: Provides an AirC2IS instance hosted on server infrastructure provided by the INF004 service, including local prerequisite COTS software, configuration, version updates and continuous support.

AirC2IS client: Provides support for an AirC2IS user on NDW003 Personal Workspace - Managed Device Service to connect via web browser to an AirC2IS Server service instance.

Available on:

NATO Secret

Availability on any other NATO or national security domains is TBC upon a new service request.

Service prerequisites:

NDW002 NATO Digital Workplace Service (High Side)/ NDW003 Personal Workspace - Managed Device Service to. AirC2IS clients require this service, which provides a standard NATO workstation connected to the NATO networks on which the AirC2IS web client application can be accessed.

INF004 - Infrastructure Virtualization Services to provide the server instances (either physical or virtual) on which the AirC2IS Server components can be deployed.

Standard Service support levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)

Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request the APP061 service please complete the Customer Request Form and contact NCI Agency Demand Management.

https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall AirC2IS availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

AirC2IS functional component	Target Availability	Performance threshold (initial access time)	Remarks
AirC2IS Mission Application (AMA)	≥ 99.5%	30"	User should be able to access AirC2IS Mission Application (AMA) within 30 sec.
AirC2IS SharePoint Information Portal (AIP)	≥ 99.5%	20"	User should be able to access AirC2IS within 20 sec.
AirC2IS System Management Application (SMA) Access	≥ 99.5%	20"	FAS Managers, Data Managers, and System Administrators should be able to access the SMA within 20 Sec.
AirC2IS Legacy System Adapter (LSA) Availability	≥ 99.5%	N/A	LSA is AirC2IS backend interfaces component not

			visible to the user.
Defence Design Save Time	≥ 99.5%	30"	AirC2IS users should be able to save the AirC2IS Defence Design of up to 1000 data elements within 30 Sec.

KPIs implementation:

AirC2IS contains internal monitoring functionality. The necessary changes to expose the above availability KPIs are planned for implementation as part of the product roadmap.

Service Restoration:

Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1013	AirC2IS User
A1014	AirC2IS System Administrator
A1025	Situational Awareness with AirC2IS
A1026	Portal and Data Management of AirC2IS
A1027	BMD Planning with AirC2IS

Service Cost / Price: Unit of measure used for service quantification for each flavour can be found in the table below:

Service ID	Service Name	Service Flavour/Option	Service Unit
APP061	AirC2IS Application Service	NCS-wide AirC2IS software maintenance and in service support	1
APP061	AirC2IS Application Service	AirC2IS client	Per user

Service ID	Service Name	Service Flavour/Option	Service Unit
APP061	AirC2IS Application Service	AirC2IS server	Per instance (standard high availability AirC2IS server cluster)

APP065 Joint Tactical Simulation (JCATS) Application Service

Service ID: APP065

Service Name: Joint Tactical Simulation (JCATS) Application Service

Portfolio Group: Application Services

Service Description: The Joint Tactical Simulation Application Service supports exercise control organisations in maintaining a virtual situation of the battle space consistent in time and space in accordance with the decisions taken by the training audience and with the activities of other relevant actors in the synthetic world at a tactical level of decision-making. The tool used for the Joint Tactical Simulation service provides the Joint Conflict and Tactical Simulation (JCATS) system which is a US Government-Off-The-Shelf simulation application with a tailor-made interface application that supports the distributed and collaborative execution of training audience orders and exercise control guidance in a synthetic world. JCATS maintains the status of the synthetic environment and all represented joint forces in time and space.

Value Proposition: This application service supports exercise designers and control organisation in gathering and in managing all the detailed synthetic data that is required to realistically produce information flows towards the training and its supporting command and control applications in a manner that is consistent in time and space based on the activities and capabilities of deployed forces. The application service allows the many contributors to the preparation and execution of a computer assisted exercise (CAX) to perform their tasks in a distributed and collaborative manner. It adds value to the CAX preparation and execution process by:

- Providing support for a collaborative and distributed way of collecting all relevant ORBAT data in an efficient manner.
- Providing support for tactical levels of information to meet the requirements of the exercise training audience.
- Providing a very broad set of automated behaviours that allow the state of the synthetic world to be maintained in an automated manner.
- Providing the ability to capture execution data and re-using it for after-action-review processes.

Service Features: The Joint Tactical Simulation Application Service offers the following features:

- Capture and manage detailed information about entities that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity in a crisis response or collective defence context.
- Manage the behaviour of entities in time and space that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity including intelligence, logistics and combat aspects.

- Provides support to produce detailed information output about entities that are relevant to the conduct and context of NATO major and small operations at various levels of intensity in a crisis response or collective defence context.

In addition, the agency maintains a JCATS ORBAT Builder (JOB) application that supports exercise planners in building that part of the ORBAT for which they are responsible in a stand-alone manner in a format that is compatible with JCATS. An exported ORBAT file can be consolidated into a central JCATS exercise dataset by the exercise database developers.

Service Flavours: The Service is available as a single flavour.

Available on:

Mission Secret or NATO Secret on locally provided infrastructure

2 Service Delivery Points on NATO Secret on centrally provided infrastructure

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: OTH001

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP066 Joint Operational Simulation Application Service

Service ID: APP066

Service Name: Joint Operational Simulation Application Service

Portfolio Group: Application Services

Service Description: The Joint Operational Simulation Application Service supports an exercise control organisation in maintaining a virtual situation of the battle space consistent in time and space in accordance with the decisions taken by the training audience and with the activities of other relevant actors in the synthetic world at an operational level of decision-making.

The Commercial-Off-The-Shelf simulation application adopted for this purpose is a sub-set of the modules provided by the Joint Theater Level Simulation (JTLS)¹. The service features a distributed and collaborative preparation of scenario data, execution of training audience orders and exercise control guidance in a synthetic world and the capture of after-action-review data. JTLS maintains the status of the synthetic environment and all represented joint forces in time and space in an internal structure as well as in an externally accessible format.

Value Proposition: The Joint Operational Simulation Application Service supports exercise designers and control organisations in gathering and in managing all the detailed synthetic data that is required to realistically portray joint operations at an operational level across the spectrum of military operations. The application service allows the many contributors to the preparation and execution of a computer assisted exercise (CAX) to perform their tasks in a distributed and collaborative manner. It adds value to the CAX preparation and execution process by:

- Providing support for a collaborative and distributed way of collecting all relevant ORBAT data in an efficient manner.
- Providing support for the controlled simulation of joint operations at an operational level of detail across the spectrum of military operations.
- Providing a very broad set of automated behaviours that allow the state of the synthetic world to be maintained in an automated manner.
- Providing the ability to capture execution data and re-using it for after-action-review processes.

Service Features: The Joint Operational Simulation Application Service offers the following features:

- Capture and manage aggregated information about entities that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity in a crisis response or collective defence context.
- Manage the behaviour of entities in time and space that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity including intelligence, logistics and combat aspects.

- Provides support to produce aggregated information output about entities that are relevant to the conduct and context of NATO major and small operations at various levels of intensity in a crisis response or collective defence context.
- Providing access to its state information to external data consumers.

Service Flavours: The service is available as a single flavour.

Available on:

Mission Secret or NATO Secret on locally provided infrastructure managed remotely¹

Two Service Delivery Points on centrally-provided infrastructure managed remotely

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: PLT008, OTH001

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

¹ The included JTLS modules are: DDS, SIP, ICP, CEP, JODA, JXSR, OMA, XMS, SYNAPSE, WHIP, SDC, OEC, AARC, OVT, ATO-T

APP067 RECCEN Application Service

Service ID: APP067

Service Name: Record Centre (RECCEN)

Portfolio Group: Application Services

Service Description: The Service provides the collaborative information management capability for Records Management, with functionalities for record keyword tagging, storage, search and retrieval. The highest content classification of records stored is limited by the security accreditation of the respective network the service is deployed on.

Value proposition: The Service offers the customers the benefit to easily access and maintain records information by providing information access control, locating and retrieval of records.

Service Features:

The Service offers the user:

- Upload of documents
- Document validation by the Registry as a "Record"
- Meta tagging of the records
- Records classification enforcement
- Records categorization
- Access control
- Browsing of records
- Search, discovery and retrieval of records
- Providing permanent links to records.

Service Flavours: The service is available as a single flavour.

Available on:

	PUBLIC	UNCLASSIFIED	RESTRICTED	SECRET	MISSION SECRET
REACH			X*		
Bi-SC AIS				X*	
Federated Access (NR)			X**		
Federated Access (NS)				X**	

Service prerequisites:

* WPS006 REACH Mobile Workplace Service / NDW002 NATO Digital Workplace Service (High Side)

WPS003 Enterprise User License Service (or any other valid SharePoint Client Access License (CAL))
PLT003 Web Hosting Service

Standard Service support levels:

Service Availability Target: 99%

Service Restoration Priority: P3.

The Standard Service support comprises the following activities:

- **Operation:** application monitoring, log management, batch jobs management, backup & restore, auditing, Service Requests fulfilment.
- **Corrective Maintenance:** diagnosis and removal of the causes and the effects of any malfunction affecting the Service.
- **Preventive Maintenance:** preventive actions needed to avoid future malfunctions
- **Adaptive Maintenance:** adjustment of the Service in order to adapt to the minor changes of the sub system components (i.e. Operating System, Database Management System, Browser, SharePoint and SharePoint add-ons). Major changes of the sub system components shall be requested via dedicated projects.

Service Cost / Price:

The unit of measure for the Service is “per user”. Since the Service is designed for the general use by all the users of each customer, the number of user will be based on the principal numbers equivalent to the sum of the “NATO Peacetime Establishment (PE)” users plus the “NATO Non-Peacetime Establishment (NPE)” users as per SOR/MER 2023.

For customers not listed in the SOR/MER 2023, the number of users will be based on the agreed number of prerequisite WPS002 units in relevant SLA/SSP.

The cost of the Service does not include the cost of all the underlying Service prerequisites.

APP068 Advisor Network (ANET) Application Service

Service ID: APP068

Service Name: Advisor Network (ANET) Application Service

Portfolio Group: Application Services

Service Description: The Advisor Network (ANET) Application Service provides services for planning, coordinating, reporting, analyzing and archiving partner engagements. Originally designed to support Advisors engaging partner nations in the scope of Train Advise and Assist missions, it has been since also enhanced to a broader context of stakeholder engagement managements. It provides an audit trail of past engagements and people, as well as the ability to assess additional elements such as partner capabilities, engagement coverages and mission objectives. It provides capabilities commonly found in Customer Relationship Management (CRM) tools, while strongly tailored to support NATO-specific requirements.

Value proposition: The ANET Application Service is an online tool (web-based) to support users when planning, coordination and reporting partner engagements. Over time, an audit trail of past engagements and partners is build up in ANET's database. ANET's advanced search and visualisation capabilities make it easy for advising organizations and mission leadership to gain context on engagements which can shape future decision making.

Service Features: ANET is a web-based tool with the following features:

- Record, collate and store engagements
- Plan and coordinate future engagements
- Gain and maintain partner relationships on both organisational and personal levels
- Assess partner personal and organizational capabilities, mission objectives and progress
- Understand and improve engagement coverage
- Advanced search, analytics and visualisation capability including GIS

Service Ordering and Request: This service can be requested via a Customer Request Form.

Service Flavours:

- APP068-1 ANET Product Lifecycle Support: This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of the specified application. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year.
- APP068-2 ANET Instance: This flavours provides for a single running copy (instance) of an application on specified network domain with its own specific setup, configuration and user access. This includes the hosting infrastructure and platform of the instance on specified network domain, the maintenance and support for the infrastructure, platform and running instance, such as OS upgrades and application upgrades and hot-fixes, and backup and recovery management.

- APP068-3 ANET User Support Small: This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 100 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.
- APP068-4 ANET User Support Medium: This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 250 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.
- APP068-5 ANET User Support Large: This flavour offers user access management and user support for all levels of users. The flavour applies to one site with more than 250 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.

Available on:

Internet
NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side) – for application instances installed on NCI Agency managed networks.

Standard Service support levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, depending the SLA for the hosted environment, the service restoration period for a critical incident (i.e.1 P0/P1) will be between 4 hours and 72 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price:

The cost of this service is composed of a product life cycle support cost which is a necessary cost to keep the product running regardless of the number of sites running the application, the product lifecycle support unit of measure is unit 1 . There is also a cost for deployment and support flavours depending on the size of the site, the unit of measure for these flavours is per site . The cost details are listed in the service rate section of this catalogue release .

APP069 Air Integrated Training Capability (ITC) Application Service

Service ID: APP069

Service Name: Air Integrated Training Capability (ITC) Application Service

Portfolio Group: Application Services

Service Description: The Air Integrated Training Capability (ITC) Application Service supports air commands exercise control organisations in maintaining a virtual situation of the battle space consistent in time and space in accordance with the decisions taken by the training audience and with the activities of other relevant actors in the synthetic world. In addition the service supports the exercise control organisation in generating relevant and compatible information flows to the training audience automated air command and control systems and in extracting structured order information from those systems. ITC provides a separate version that has been extended with specific models and behaviours for Ballistic Missile Defence (BMD) sensors, weapon systems and threats. ITC (BMD) interacts with the APP059 Joint Exercise Management Module (JEMM) for scenario preparation, execution and interoperability.

Value Proposition: The ITC application service supports exercise designers and control organisation in the air C2 community in gathering and in managing all the detailed synthetic data that is required to realistically produce information flows towards the training audience and its supporting Air C2 systems. The application service allows the many contributors to the preparation and execution of an Air C2 computer assisted exercise (CAX) to perform their tasks in a distributed and collaborative manner. It adds value to the CAX preparation and execution process by:

- Providing support for a collaborative and distributed way of collecting all relevant ORBAT data in an efficient manner using a familiar interface.
- Providing interoperability with NATO Air command and control systems in an efficient and flexible manner.
- Providing a very broad set of automated behaviours that allow the state of the synthetic world to be maintained in an automated manner.
- ITC (BMD) integrates with JEMM to provide the simulation of BMD scenarios either as a stand-alone capability or in combination with other simulations through the DIS protocol.

Service Features: The ITC system is built upon a Commercial-Off-The-Shelf simulation framework (FLAMES). ITC provides an air exercise control organisation with the ability to simulate air operations as defined in an Airspace Coordination (ACO) and Air Tasking Order (ATO) for two opposing and one neutral side. An exercise controller can manage the overall execution of the scenario and influence the adjudication of simulation outcomes. The resulting status updates are fed automatically into the Integrated Command and Control (ICC) in the form of air tracks, status updates and messages. ITC (BMD) integrates with JEMM to provide the simulation of BMD scenarios and produce shared early warning and Link-16 tactical data links either as a stand-alone capability or in combination with other simulations through the DIS protocol.

Service Flavours: The Service is available as a single flavour.

Available on:

Mission Secret

NATO Secret

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

APP059 Joint Exercise and Management (JEMM) Application Service for ITC (BMD)

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1015	Integrated Training Capability (ITC) Technical Control Officer (TCO)



Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP070 Training Objective Development and Management (TOMM) Application Service

Service ID: APP070

Service Name: Training Objective Development and Management (TOMM) Application Service

Portfolio Group: Application Services

Service Description: The Training Objective Development and Management Application Service supports exercise training audiences and associated training organisations in producing a structured and prioritised set of training objectives for a particular training event and phase in a collaborative and distributed manner according to the process in the Bi-SC Directive 75-3. An organisational set of reference training objectives can be maintained and used as the basis for the development of exercise-specific training objectives.

In addition, the application service supports exercise training audiences and associated training organisations in managing training objective resource conditions in a distributed and collaborative management according to the guidance described in the Bi-SC Directive 75-3 throughout the exercise preparation phase.

Value Proposition: This application service supports exercise training objective owners and supporting resource condition owners in developing training objectives according to the Bi-SC Directive 75-3 in a structured manner. It adds value to the process of developing and managing training objectives by:

- Providing the ability to manage a set of reference training objectives
- Providing support for a collaborative and distributed way of working.
- Providing support for the workflow between the stages of development.
- Providing an explicit statement of resource requirement and acknowledgment by resource owner.
- Providing a real time up to date dashboard of the state of achievability of training objectives throughout the exercise planning and preparation process
- Reducing travel and coordination effort.
- Enabling a wider participation in the process by training audience personnel and resource owners.

Service Features: The features of the Training Objective Management Module (TOMM) are:

- Act as an organisation training objective manager to create, update and delete reference training objectives including resourcing conditions.
- Act as a Training Objective Manager capable of managing the contributions and workflow of the TO development process including the prioritisation
- Act as Training Objective Scripter capable of defining the content of training objectives, the associated resourcing conditions and standards
- Act as a resourcing condition owner capable of commenting and acknowledging resource requirements.

- Develop training objectives according to the stages and format specified in the Bi-SC Directive 75-3.
- Review training objectives and associated resource conditions in a collaborative and distributed manner
- Manage and track the achievability state of the training objective resourcing conditions.
- Prioritise training objectives and re-organise their sequence accordingly.
- Review and update the achievability of resource conditions in a dashboard until the start of the exercise.
- The TOMM training objectives are fully compatible with the training objectives of APP059 JEMM.

Service Flavours: The Service is available as a single flavour.

Available on:

Mission Secret
NATO Secret

Service Prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: PLT008, OTH001

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A5003	Training Objective Management Module (TOMM)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP071 Enterprise Business Application (EBA) Service

Service ID: APP071

Service Name: Enterprise Business Application (EBA) Service

Portfolio Group: Application Service

Service Description: The EBA service is built as an integrated system of systems tailored to support a number of enabling processes for day-to-day operational activities of the NATO C&I Agency processes. The service can be offered as-is as an extension of the operational service defined for the NATO C&I Agency through the execution of a project. Alternatively, the service can be replicated and adapted to meet specific customers' needs subject to proper analysis and implementation through a fully funded project.

Value Proposition: The Service is designed and implemented to support a defined set of processes currently in place at NATO military and civilian organisations. It meets the requirements defined for customer funding regime and the relevant NATO committees. It is operational and used by NCI Agency and can be extended, deployed and adapted to any NATO body or national entity.

Service Features: The Service provides support to:

- All financial processes in line with IPSAS;
- Full acquisition processes including the direct interaction with the industry for ordering services and supplies;
- NATO specific Travel process;
- Most of the HR processes;
- Management of assets (ICT and non-ICT);
- Full P3SM process to manage Portfolio, Programs, Projects, Services and Resources;
- Reporting for each function/process area;
- Enterprise Reporting (Business Intelligence) across functional/process areas.

Service Flavours: The Service can be tailored to include only specifically required features to meet specific customer needs.

Available on: The service is available on NU with some elements on NR.

Service Prerequisites: Access to NATO NU/NR.

WPS006 REACH Mobile Workplace Service

NDW001 NATO Digital Workplace Service (Low Side)

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP072 Core Financial System (CFS) Application Service

Service ID: APP072

Service Name: Core Financial System (CFS) Application Service

Portfolio Group: Application Service

Service Description: COTS-based service offering a system that supports standard & IPSAS financial processes used in NATO.

Value Proposition: Service configured to support project implementation and lifecycle for medium to large projects, thus enabling financial and accounting administration of projects in an effective and efficient manner.

Service Features: The service covers requisition, purchasing, project accounting, payments, General Ledger, and reporting. It supports standard financial, procurement, payment, and reporting functions belonging to a COTS-based financial system.

Service Flavours: The Service is available as a single flavour.

Available on: NR

Service Prerequisites: The Service requires virtual servers configured to enable functioning of the Oracle PeopleSoft Financials 8.4.

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP074 NATO Lessons Learned Portal (NLLP) Application Service

Service ID: APP074

Service Name: NATO Lessons Learned Portal (NLLP) Application Service

Portfolio Group: Application Services

Service Description: The NATO Lessons Learned Portal Application Service supports the Lessons Learned communities in sharing and searching through lessons learned data, in tracking the progress of the staffing of observations, in managing the user accounts, roles and access, and in managing portal meta-data through a concept of data dictionaries. The Service supports NLLP managers, Lessons Learned Community of Interest (COI) site administrators, lessons learned facilitators, and regular NLLP users in:

- Tracking the progress on the NATO Lessons Learned process of specific observations;
- Managing the users and their access and rights to collaboration sites;
- Managing collaboration site metadata;
- Managing shared COI-specific collaboration sites with dedicated search metadata, with document libraries and event information.

Value Proposition: The Service is an essential enabler of a more effective and efficient NATO Lessons Learned process.

Service Features: The Service provides the following features to NLLP users:

- Creation and management of COI shared sites, including exercise event sites (NATO EXTRA COI);
- Management of metadata for COI shared site searches;
- Management of metadata for the lessons learned document searches;
- Integration with authenticated classified windows domain users;
- Management of membership users and roles;
- Access through forms-based solution;
- Assignment of users to NLLP application roles: site collection managers, NLLP managers, lessons learned facilitators, and NLLP users;
- Distinction of COI users into owners, members, and visitors;
- Facilitation of the NATO Lessons Learned Process workflow through:
 - Adding observations;
 - Maintenance of the lessons status;
 - Provision of the automated mail notifications;
 - Tracking of progress from noted, potential best practice, lessons learned, and best practice stage;
 - Archiving of lessons learned data;
- News pages;
- Conversion of the lessons learned data into PDF format documents to enable sharing;
- Storing and provision of the lessons learned documents;

- Management of specific site related to lessons learned related events and activities;
- Access to usage data collection datasets in a standardised and documented manner

Service Flavours: The Service is available in two flavours:

The full NLLP – includes all the features of the Service, including the tracking of lessons learned;

Public NLLP – includes all the features of the Service, except the tracking of lessons learned.

Available on:

NATO Unclassified
NATO Secret

Service Prerequisites:

Windows server 2016
SQL Server 2016
SharePoint Server 2016
IIS 8.5. for NCS users

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: for NCS customers, the restoration priority will be as specified in centralised or local service level agreement.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP075 Electronic Warfare Functional Services (EW-FS) Application Service

Service ID: APP075

Service Name: Electronic Warfare Functional Services (EW-FS) Application Service

Portfolio Group: Application Services

Service Description: The EW-FS Application Service provides an integrated, robust, and flexible capability supporting a suite of services available throughout the Bi-Strategic Command (Bi-SC) Automated Information System (AIS) to address the NATO's emitter data management processes and dissemination of EW information in a timely and responsive manner in accordance with NATO policy, doctrine, and guidance. It is as a web-based capability, with advanced data storage, and near-real time data sharing capabilities, deployable in a federated infrastructure of system of systems. The Service includes Increment 1 of Electronic Warfare Functional Services (EW-FS), and it is implemented through the NATO Emitter Database – Next Generation (NEDB-NG) application. The capability can adequately describe modern complex emitters, which continue to proliferate within the electromagnetic environment and it supports the automation and integration with other information capabilities.

Value Proposition: The Service provides the NATO Electronic Warfare Community with a capability to achieve the following operational benefits:

Increment 1 (NEDB-NG)

The Service provides the NATO Electromagnetic Warfare Community with a capability to achieve the following operational benefits:

- Support to NATO's emitter data management processes.
- Sharing of emitter information and data across NATO at all levels of command.
- Enhancement of the emitter information dissemination to Nations and other domains.
- Coordination between data providers through the Active Task mechanism.
- Contribution to the development of the initial Electromagnetic Order of Battle (EOB).
- Provision of the search and analytical capabilities to retrieve/analyse emitter information.
- Provision of specialised functionalities in support of specific domains: radar electro optical and communication externals.
- Support to interoperability with external systems.
- Deployment in a federated infrastructure of system of systems, including classified networks and standalone machines.
- Management of Users and Permissions.
- Support to all operational mission types.

Increment 2 (C2 of EW)

C2 of EW Functional Services will achieve the following Operational benefits:

- Increased tempo and accuracy to outcompete adversaries.
- Increased integration across warfighting functions and domains.
- Increased capacity to mitigate threats and exploit opportunities.
- Increased effectiveness across the range of operations.
- Increased Day Zero Readiness.
- Improved process standardisation among Allies and partners.
- Increased automation and staff effectiveness.

Service Features: The following functional services, are provisioned through EW-FS:

Increment 1 (NEDB-NG)

- Emitter Services

Increment 2 (C2 of EW)

- Recognised Electromagnetic Picture (REMP) Services.
- Electromagnetic Order of Battle (EOB) Services.
- Electromagnetic Warfare Planning Services.
- EW Direct, Monitor & Assessment Services.
- Emitter Analysis Services

Service Ordering and Request:

Increment 1 (NEDB-NG)

ACO Service Level Agreement defines availability of services. CRF may be submitted for requests outside of SLA.

Increment 2 (C2 of EW)

Services not initially available outside of scope defined in ACO Service Level Agreement. Further expansion may become an option in the future.

Service Flavours: EW-FS supports different flavours depending on the operating environment and connectivity:

Increment 1 (NEDB-NG)

- Scorpio Standalone Read-Only deployed on stand-alone secure laptops to provide offline read-only access to emitter data.
- Scorpio Standalone Read-Write deployed on stand-alone laptops to provide offline read-write access to emitter data.
- Scorpio National Master – Deployed on server systems to provide online access and updating of emitter data on national networks.
- Scorpio NATO Master – Deployed on server systems to provide online access and updating of emitter data on NATO and BICES networks.

Increment 2 (C2 of EW)

- C2 of EW – is initially available exclusively on the NATO AIS Network.

Available on:

NATO Secret

Service Prerequisites:

INF004 Infrastructure Virtualization Service
PLT008 - NATO SOFTWARE FACTORY
PLT014 - Integration and Testing Platform Service

Underlying Services: PLT008, OTH001

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration:

Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 8 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised CSLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP076 Indications & Warnings (I&W) Application Service

Service ID: APP076

Service Name: Indications & Warnings (I&W) Application Service

Portfolio Group: Application Services

Service Description: The Indications & Warnings (I&W) Application Service provides a portal for the intelligence watch community, with a tool enabling monitoring of indicator statuses and sharing of warning intelligence.

Value Proposition: The Service provides the NATO Intelligence Community with a capability that enables management, access to, contribution, visualisation, reporting, and repository of relevant indicators.

Service Features:

- A comprehensive I&W indicators and reports search capability;
- Creation, upload, and management of warning reports;
- Color-coded Watch Conditions (WATCHCON);
- User-updatable indicators, sub-indicators, and their definitions;
- User-updatable links and supporting documents;
- User-configurable news and newsfeed system.

Service Flavours: The Service is available as a single flavour.

Available on:

- NATO SECRET
- BICES Network

Service Prerequisites:

- PLT001 Information Sharing and Collaboration Platform Services
- PLT003 Web Hosting Service

Underlying Services: OTH001

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP078 ORION Space Domain Application Service

Service ID: APP078

Service Name: Orion Space Domain Application Service

Portfolio Group: Application Services

Service Description: The Orion (Space Domain System) Application Service provides an integrated and flexible capability supporting Space Support in Operations services throughout the Bi-Strategic Command (Bi-SC) Automated Information System (AIS). Orion provides a centralised location for up-to-date Space Domain information (Space Domain Awareness), ensures the dissemination of operational Space support information (Operational Space Support) in a timely and responsive manner, and facilitates the coordination of Space actions with the other operational Domains (Space Domain Coordination), in accordance with NATO policy, doctrine and guidance.

Value Proposition: Orion provides the NATO Space Operational Community with a capability that enables the following operational benefits:

- Provides a knowledge management of Space-related documentation, systems and resources for the NATO space community and space data and product users in NATO.
- Enables allows requesting and sharing space data, products and services across NATO and Nations at all levels of command to enable Multi Domain Operations.
- Manages the access and dissemination of space support information from the NATO Space Operations Centre to the requestors.
- Provides daily Space information, including daily SDA updates from the NATO Space Operations Centre, TLEs, orbital change likelihood, etc. across the 7 Space functional areas (e.g., SATCOM, ISR, PNT, SSA, METOC, SEW, Space Security)
- Provides an inventory of Space assets and their capabilities, as well as Space threats, with search and analysis functions, (blue and red assets).
- Provides up-to-date information on Space events and NATO and National Space points of contact.
- Provides structured Space Domain reference documentation, including for multinational initiatives (e.g., APSS), and other programmes related to the Space Domain (e.g., NDPP, Space COE, etc.)
- [new] Enables dynamic the procurement of space data and service and derivative products from commercial providers (e.g. satellite data, analytics), its normalization, cross-domain upstream transfer, and integration in the space domain awareness picture.
- Enables and tracks ACO requests for space support from NATO nations
- Supports interoperability with external systems.
- Manages Users and Permissions.
- Supports all operational mission types.

Service Features: The Orion Application Service is comprised of the following features that combined support the three key tasks of the Space Operational Community:

- Provides a system to request, approve and monitor Space Support Requests (SSRs).

- Intelligence management. Provides the operational community with up-to-date Space-related intelligence information (including counter-Space).
- Intelligence Processing – creation/management of intelligence products on RED Space capabilities, such as Space Order of Battle (ORBAT)

Service Flavours: The Orion Application Service can be customized and adapted to the requirements of the operational community.

- [new] Space domain data exploitation suite: planning, data management, automated pipelines, exploitation client, SOM creation.
- [new] Space domain awareness data service acquisition: vendors management, bidding process, contracting, data-management.

Available on:

NATO Secret

Service prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: PLT008, OTH001

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP079 NATO Automated Biometrics Identification (NABIS) Application Service

Service ID: APP079

Service Name: NABIS Application Service

Portfolio Group: Application Services

Service Description: The NATO Automated Biometrics Identification System (NABIS) is designed to support the NATO Biometrics capability by enabling the user community to safely exchange biometric data in a NATO Joint Operations Area (JOA), between JOAs and beyond the operational context. The NABIS supports the full spectrum of the military operations, from tactical to strategic level, and can make a critical contribution to removing anonymity from threat actors.

Value proposition: Biometric capture and data interchange in the multi-national operational environment is something that has posed a great challenge to NATO operations. NATO has no effective means by which to assist the Nations to share data in a flexible yet interoperable way. NABIS has been developed to address and mitigate this shortfall, as follows:

- establishes a data sharing environment on the BICES/ NS WAN networks enabling the exchange of biometric data amongst participating NATO nations;
- enables and promotes biometric interoperability, biometric data sharing, as well as provides biometric capability for participating NATO nations that do not have their own national system;
- NABIS is a web application that allows storage, search, retrieval and dissemination of biometric data. It used a commercial engine to support automated matching of three modalities (Face, Fingerprint and Iris);
- it has an robust architecture, which can be easily extended with new functionalities or connections to other external matching engines;
- NABIS implements NATO STANAG 4715 compliant format for the exchange of data with other ABISs or enrolment devices and has functionality to import and export data from and to other biometric formats such as the USA Department of Defence (DoD) and Federal Bureau of Investigation (FBI) Electronic Biometrics Transmission Specification (EBTS).
- provides biometric and biographic data upload, which allows national ownership as defined in NATO standards (STANAG 6515 and STANAG 4715);
- uses web services to support “Ping and Ring” networks between multiple ABIS systems;
- provides a technical solution to manage Persons of Interest (PoI) included in the JOA Biometrics Enabled Watchlist (BEWL);
- supports the vetting process of the Locally Employed Personnel (LEP) in both static and deployed environments;
- contributes to Identity Intelligence (I2), Human Network Analysis in support of Targeting (HNAT), Force Protection and Counter Intelligence.

Service Features: NABIS is comprised of the following essential features:

- imports and stores biometric enrolments (i.e. fingerprints, face and iris) as well as latent prints from both collection devices and other ABISs;

- conducts automated searches of a newly imported/ received biometric file against the entire data base;
- performs an automated match/ no match decision based on pre-set thresholds and matching scores;
- provides a list of candidates sorted on the fused matching score, which supports further examination of face and latent images;
- it is NATO STANAG 4715 compliant;
- imports data from enrolment devices or other data collection and storage systems;
- shares biometric files through “Ping&Ring” transactions with networked ABISs, which allows for exchanging architecture where each participant retains the ownership of their data;
- enables management of Pol on the BEWL.

Service Flavours: NABIS supports Biometric Operations by storing, comparing, matching and disseminating three biometric modalities – fingerprints, face images and iris images. Within NABIS, data is grouped in two main categories based on how the biometric modalities have been collected: (a) enrolments, which includes the enrolled fingerprints, face and iris and (b) latent, which contains the latent prints collected from various objects. The NABIS also displays the JOA BEWL through a dedicated folder. The NABIS allows for advanced searches based on contextual information as well, and for saving the searches for accessing any potential updates. Likewise, it allows for subscriptions, which enables the user to be notified by emails whenever a new data matching the subscription was received in the system.

Available on:

NATO Unclassified (Training and exercise only)
NATO Secret WAN
BICES

Service prerequisites: NABIS is a fully web based application that requires a server installation. Client machines only require a HTML5 compatible browser like Chrome or IE11 or later.

Underlying Services: PLT008

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP081 Joint Advanced Distributed Learning (JADL) Application Service

Service ID: APP081

Service Name: Joint Advanced Distributed Learning (JADL) Application Service

Portfolio Group: Application Service

Service Description: JADL Application Service and Support provides users across the Alliance the ability to access and deploy e-learning. In addition, it provides help desk services for all users.

Value Proposition: This service includes the offering of a Learning Management System (LMS) to NATO (-partner) Nations. By leveraging this platform, users can decrease delivery costs and increase speed of delivery of online training. Moreover, JADL provides detailed analytics about the learning process, completions and scores of individual users, as well as groups. So by making use of JADL, customers can make sure their audiences are trained for a specific task faster, and for less money. Services include hosting the learning management system and managing the help desk for all users.

Service Features:

For end-users (individual learners):

- Provides access and consume e-learning modules
- Provides certificates after successful completion
- Provides helpdesk support to all users

For NATO entities (commands, Nations etc.) deploying online content on JADL

- Manages content on JADL
- Provides reporting and analytics

The helpdesk support will have the following characteristics (all included in one package, no cost differentiation between support levels):

- *Level 0: Self-service:*
Guidance / micro-learning in JADL about basic features so users can trouble-shoot themselves, and prevent tickets in the first place
- *Level 1: Basic helpdesk support*
Support basic issues in the start-to-end process: access, account request, approval, login, search for course, join course, course progress, certificates.
Support more complex and non-standard issues + managing *content*, e.g. modules that won't play (troubleshooting and fixing needs to take place in the SCORM package /module itself, not in the LMS), uploading and testing new courses, removing obsolete content, generating reports for specific customers etc.
- *Level 2: Advanced help desk support*
Support to solve deeper engineering issues in the platform itself.

Service Ordering and Request:

The customer requests the service through the ACT ESMA and users request support through an institutional email inbox. The implementation of an internet-facing ticketing systems is underway.

Service Flavours: N/A

Available on:

NATO Unclassified

NATO Secret

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)

Underlying Services: PLT008

Standard Service Support Levels:

Service availability target: 99.0% (TBC)

Service Restoration: Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

- Critical Issues (System Down, Major Functionality Loss):
 - Restoration within 4 hours for any critical issues, with clear communication throughout the restoration process. This includes a full resolution or, at a minimum, a workaround to minimize disruption.
 - In the case of an extended outage, provide regular updates every 30 minutes to keep stakeholders informed.
- High-Priority Issues (Major Impact on a Large User Group, but Not System-Wide):
 - Addressed and restored within 6 hours. Communication during the restoration process is essential, with users kept informed of progress and expected resolution timelines.
- Medium-Priority Issues (Individual User Access, Minor Features Affected):
 - Resolution within 1 business day. While individual user cases may take longer, a clear plan will be in place to address them promptly.
- Low-Priority Issues (Non-Urgent, Cosmetic Issues):
 - Resolved within 2-3 business days, depending on complexity and resource availability.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP082 Digital Emergency Alert Notification Service

Service ID: APP082

Service Name: Digital Emergency Alert Notification Service

Portfolio Group: Application Services

Service Description: The Digital Emergency Alert Notification Service provides customers with timely emergency alerts and mass notifications which can be sent to target audiences or broadcasted in mass to users on NATO Networks; as well, to the community members. The service enhances security and situational awareness with comprehensive enterprise class alerting essential to crisis response and civil communications.

Value Proposition: The service offers intelligent emergency communications distribution combined with guaranteed content delivery. Furthermore, it allows for the placement of methods, functions and triggers that interact with and bring crucial data to and from end-users; based on end-user and/or management's predefined business rules and settings. The Service provides seamless integrations with enterprise-class federated environments and shares communications and commands using standardized HTTPS, XML, HTML, SMTP protocols.

Service Features: The Service is installed as a client application on Managed Devices and when activated by "push" notifications from "notification moderators", the user receives a near real-time Pop-Up notification box where a pre-defined or custom tailored message can be seen. Includes a fully managed VM centrally hosted, a web-based server application solution secured with the appropriate posture for use on NATO Networks. The Service approach is based on applications that work in tandem with stakeholders to deliver a comprehensive solution.

Features and Options include:

- Templates: create and save alert templates for future use
- Scenarios: create alerts in advance for rapid activation manually or automatically
- Pre-scheduling of alerts for release at scheduled date and time
- Scheduling of recurring alerts
- Built-in capability for scrolling banner text computer alerts
- Sizing of computer alerts from small to full screen display
- Text-to-voice feature automatically reads the computer alert out loud
- Each user may have multiple email addresses, multiple phone numbers, multiple SMS numbers, multiple keywords, multiple groups, multiple roles

Service Flavours: The service is offered as a single flavour.

Activities in scope of service:

- Service management of entire service lifecycle including regular user communication;
- Requirements analysis and validation with the customer:
 - Propose technical solution;
 - Evaluate and propose costs based on requirements and technical solution;
- Application management:

- Incident Management:
 - Issue Investigation and Resolution; Escalation of tickets to 3rd party supplier when required and follow up until their final resolution;
- Independent Verification & Validation:
 - Change Configuration Proposal (CCP) Submission and Follow up;
- Deployment:
 - Configuration & Reconfiguration;
 - Deploying & Release, and Patches Management;
- Operations:
 - Operate and perform the required maintenance on the application servers and the underlying platform;
 - Set up and Maintenance required Reference/Test and Development environment in NSF and make it available for the customer.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Public Cloud

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side) / WPS006 REACH Mobile Workplace Service
WPS002 Enterprise Identity Access Management Service

WPS016 Enterprise Managed Mobility Service

Underlying Services: PLT008, SME005

Standard Service support levels:

Service Availability Target: N/A

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is 'per managed device'. Please see Service Rate document for the price details.

APP083 Mission Planning Application Service for Dual Capable Aircraft

Service ID: APP083

Service Name: Mission Planning Tool for Dual Capable Aircraft

Portfolio Group: Application Service

Service Status: Available

Service Description: The Mission Planning Tool for Dual Capable aircraft provides computer tools to aid in planning conventional and non-conventional aircraft missions. It will be based on the Joint Mission Planning System (JMPS), and will consist of computer hardware using common core software called the Joint Mission Planning Environment (JMPE). JMPS is intended eventually to support most aircraft, weapon, and sensor assets. This Service includes the maintenance of relevant operational support data e.g. maps, Digital Aeronautical Flight Information File and aircraft performance profiles.

Value Proposition: This Service will allow the user to plan conventional and non-conventional aircraft missions. It will provide a package of common and platform-unique mission planning applications that will help to increase the accuracy of the military planning cycle and will improve combat readiness.

Service Features:

- Operational Scenario management
- Pre-mission briefing
- Route planning and evaluation
- Target / objective analysis

Service Flavours:

- Stand-alone workstation
- Network based installation (VDI)

Available on: NATO Secret

Service Prerequisites: NDW002 NATO Digital Workplace Service (High Side)

Standard Service Support Levels: (std)

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial numbers:

Belgium +32 65 44 3177

Netherlands +31 70 374 3177

Italy +39 081 721 3177

Germany +49 282 4978 3177

USA +1 757 747 3177

For NATO HQ +32 02 707 5858

Service Availability Target: 99.5% Availability

Service Restoration:

Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. *Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.*

Service Cost / Price: The unit of measure for the Service is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

APP084 International Submarine Escape and Rescue Liaison Office (ISMERLO) Application Service

Service ID: APP084

Service Name: International Submarine Escape and Rescue Liaison Office (ISMERLO) Application Service

Portfolio Group: Application Services

Service Description: ISMERLO is a web based Command & Control system used to plan and co-ordinate escape and rescue efforts for the worldwide submarine community during peace time.

Value Proposition: The system enables the international submarine community to manage all submarine escape and rescue assets and elements. It enables the community to raise alerts for real or simulated submarine incidents and to help determine the quickest and most effective escape and rescue assets to use to assist with the escape or rescue activities.

Service Features:

- Time to First Rescue and Time to First Intervention C2 planning calculations.
- Real world navigational routing for support vessels.
- Vessel position updates via AIS
- SMS and email notifications of real world alerts and exercises.
- Vessel of Opportunity management.
- Submarine management.
- Rescue and intervention asset management.
- Airport & Seaport data management.
- Medical data management.
- Private and group communications.
- Forum, event and calendar management.
- Site data managed and maintained through comprehensive integrated Content Management System.

Service Flavours: One version of the system is available.

Available on: The system is available on the open internet. This is because the ISMERLO community is made up of all worldwide nations that have submarine capabilities. This includes NATO members, and also nations such as Russia, China, India and Australia etc.

Service Prerequisites: No prerequisites needed.

Underlying Services: PLT008, OTH001

Standard Service Support Levels: P3 level

All supporting and underpinning services for ISMERLO are expected to carry at least a 99.8% availability.



Service Cost / Price: The unit of measure for each of the Service Flavours is 1. The total of the NATO Service Delivery cost is charged in accordance with specifically arranged conditions of the Service Delivery.

APP085 Housing Office Management Application Service

Service ID: APP085

Service Name: Housing Office Management Application Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Available

Service Description: The Service offers our Customers an improved and effective Housing Management solution that supports properties managed by local Housing Offices, both on-base and off-premise properties, allowing consolidated management of leases and coordinate maintenance requests.

Value Proposition: The Housing Office Management Application Service serves the property management and rental flow for NATO military and civilian personnel entitled to rent on base housing in an automated and standardized manner.

Service Features: Housing Office Application includes the following Modules:

- **Register customer application** - Customer application form management and printing;
- **Customer Administration** – Search Customer; List Customers; Edit Customer Details; Add customer to waiting list; Print customer validation form;
- **Residence Administration** - Register residence; Search residence; List residence on criteria; Edit residence details;
- **Proposals Administration** - Register proposal; Print proposal/offer from template; Search customer proposals; List proposals;
- **Booking Administration** - Register booking; Print acceptance from template; Search customer bookings; List Bookings;

Service Flavours: The Service is available as a single flavour.

Available on: NATO Unclassified.

The Service may be available on other security domains upon a New Service Request.

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side)

WPS002 Enterprise Identity Access Management Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period is 8 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.



Service Cost / Price: The unit of measure for the Service is by a Database instance. Price details available in the Service Rates Document.



APP086 NATO Information Portal Application Service (NIP)

Service transitioned to NDW006.

APP087 CRC System Interface (CSI) Application Service

Service ID: APP087

Service Name: CRC System Interface (CSI) Application Service

Portfolio Group: Application Services

Service Description: The NATO Control and Reporting Centre (CRC) System Interface (CSI) is a real time Command & Control System currently in operational use in 26 NATO nations. The system, originally developed by Raytheon, has since been significantly modified and enhanced under the multi-nationally funded CSI Memorandum of Understanding. The legacy hardware has been replaced by modern Common off the Shelf (COTS) hardware and the software has been totally re-written to support today's modern operating systems.

The CSI System is used both as a Command & Control system and as a Data Link Integrator, integrating both radar feeds and tactical data links. All major data links are supported including Link 1, Link 11A, Link 11B, Link 16, ATDL-1, Variable Message Format (VMF), Cursor on Target (CoT), OTH-Gold and NATO Friendly Force Interface (NFFI).

The CSI offers integrated fighter control for directing Link 16 equipped fighters and full Ground Based Air Defence (GBAD) control. The Human Machine Interface (HMI) is a modern Java application that can either be deployed standalone or as part of an integrated MASE / CSI solution.

The CSI Local Support Service flavour includes the installation, configuration and maintenance by the CSU Staff of the CSI system in order to facilitate the 24/7 availability of the system for the operational staff at NCS Sites. A detailed description of these particular activities can be found under "Service Flavours" below

Value proposition: The CSI server is the main application. It is developed in Ada and C and provides most of the CSI System functionality.

CSI is a real time Command and Control system interfacing on ATDL-1, Link 1, Link 11A, Link 11B, Link 16, OTH-Gold, NFFI, VMF and COT. The CRC Systems Interface provides complete SAM, Link16 C2 Unit and Fighter control (Link 16 Non-C2 Air Unit) functionality into the CRCs, provides a correlated air, ground, surface, subsurface, and space picture for SAM units, Fighters, the E3A, ships, CRCs and other land units.

The primary purpose of CSI is to provide CRCs with a Fighter control and SAM control functionality and to route tactical data to any connected system. The CSI implements Threat Evaluation and Weapon Assignment (TEWA) processing; it is able to evaluate a list of the most threatening tracks against the points to be defended and it associates the best SAM/Surface system for the engagement.

The TEWA processing has been applied to fighter control in addition to GBAD control. It is possible to draw Safety Sectors and Factor Bandit Range Sectors around hostile and friendly tracks. These sectors represent the engagement volume of the fighters. Time to safety sector and time to factor bandit range inform the fighter controller about crucial timing related to fighter interception.

CSI implements pre ID and auto ID functionality based on Link 16 identities. It also implements a procedural identification evaluation based on the loaded ACO corridors.

The CSI uses the standard NATO data links Link-1, Link-11A, Link-11B, ATDL-1, Link-16 and OTH-Gold. Data exchange between the CSI System and the CRC is accomplished via the Link-1 protocol, Link 11B protocol or Link 16 protocol. This is site dependant and depends upon the interfaces provided by the host CRC. Data exchange with connected units is accomplished via Link-16, , Link11B, Link11A, ATDL-1 or OTG. Data exchange between the CSI and fighters is via the Link 16 protocol only. The CSI acts as a message translator between interfaced systems and provides the necessary communication gateway services required to reconcile incompatibilities between the referenced links.

CSI fully supports the latest Network Enabled Weapons functionality.

CSI can run in a redundant configuration where two servers are running simultaneously, one as master and one as slave. The slave server is in hot standby mode and at the event of a catastrophic failure of the master server, it takes over migrating all the connections.

Service Features: The CSI supports many different simultaneous connections (Link 1, Link 11A/B, ATDL-1, VMF, Link 16, JREAP, NFFI and OTH-Gold). For Link 16 the CSI has everything to operate both on a live Link 16 network and to connect to other Link 16 systems using normal ground infrastructure. The HMI has been completely re-designed based upon state-of-the-art techniques and tools. The functionality within the CSI system includes:

- Transmitting/Forwarding and Receiving of tactical datalink messages
(Link 16, Link 11A, Link 11B, ATDL-1, Link 1, VMF, NFFI, CoT)
- Reception and forwarding of Over the Horizon Target Gold (OTH-Gold).
- Pre ID and auto ID functionality based on Link 16 identities.
- Procedural Identification Evaluation (PIE) based on the loaded ACO corridors
- Track processing for Air Tracks, Surface tracks, Land Tracks, Subsurface Tracks, Reference Point, Emergency Points, EW Products and Space Tracks.
- Correlation/De-correlation (Air Track/Air Track, Air Track/Target, TBM/TBM)
- Filtering (Geographic/Identity/Security)
- Online Tactical Data Extraction and Monitoring
- Free Text Message exchange
- Link-16 Imagery Processing
- Link-16 Network Enabled Weapons
- Recording/Reduction and Replay
- SAM/GBAD Control and Monitoring
- Fighter Control (STANAG and MilStD) and Mission Monitoring
- TBM data provision, processing and engagement management from Link 16 and connected radars (TPS-77, RAT-31DL and SMART-L)
- Link 16 exchange on an unlimited amount of connections using various protocols (e.g. MIDS/JTRS (A, B, I, D, J, R, MOS) over Ethernet or 1553 Bus, JREAP and SIMPLE)
- Advanced JREAP (A,B and C) routing including (remote) management messages

- Multiple MIDS LVT (1,2,4,6,11) BU1, BU2, STT and JTRS Terminal Monitoring and Control
- CSI Integrated Link 16 Network Management Application (CINEMA)
- Link16 Network and Terminal Emulation
- Link 16 network design through CSI Advanced Network Design Tool (CANDIT)
- Local and Remote Link 16 Ground Equipment Suites.
- NTDS Interface Processor (NIP) for communication on Link 11A.
- Flight Plan Receiver / Flight Plan Server (From MASE Repository)
- ATO/ACO automatic and manual reception and processing.
- Threat Evaluation and Weapons Assignment (TEWA) for SAM units and fighters.

Service Flavours:

CSI software maintenance and in service support: (singleton service provided to Members of the CSI Board) Includes the development, testing, documentation and release of the CSI baseline to all sites registered for CSI. However, the sites themselves are responsible for the system update.

CSI instance installation and in service support: Upon request, CSI instances can be provided to CSI Board Members through an installation service. Such services are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

CRC System Interface (CSI) Local Support Service (INF041): The following services are provided under NCI Agency CSU Support:

1) Installation of new baseline

NCI Agency CSI section releases annual baseline updates to CSU's after the baseline has been accepted on the Approved Fielded Products List (AFPL). Upon release of a new baseline, CSU personnel will perform the baseline upgrade to install the new version of the CSI Software.

2) Adding / Modifying connections to the system

The addition of connections and the modification of connections are usually performed by CSI System Operators. However, liaison will be required with CSU personnel to ensure that the correct route exists to the connecting system and that the connection can successfully pass through any established firewalls.

3) Troubleshooting connections

Connections employed in the CSU consist predominantly of JREAP-C and Link 11B connections. Occasionally a channel may be in the failed status and CSU personnel may be requested to diagnose the data link issue to determine which system is at fault.

4) Data Archiving.

All data exchanged by the CSI System is recorded. In addition, the operational picture and operator inputs are also recorded. CSU personnel are responsible to ensure that

all data (including operational logs / system logs) are correctly archived for any future use.

Value Proposition: Use of the CSI Local Support service provides for a reliable CSI installation allowing data to be exchanged between NATO installations and national sites. The use of the service ensures the availability of the CSI system, ensures that the baseline being run is the latest available version on the AFPL and ensures that physical connections are correctly established in order to serve the data exchange requirements.

Service Features: The functionality within the CSI Local Support includes :

- Baseline installation
- System configuration
- Data Archiving
- Datalink troubleshooting

Available on:

NATO Confidential
NATO Secret
Mission Secret

The Service may be available on other networks upon a New Service Request.

For INF041, CSI Software is delivered as a NATO Restricted delivery. The installations supported by the CSI Local Support service are hosted solely on the NS-WAN.

Service prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

For INF041, the CSI runs on virtual machines provided by the CSU and therefore these virtual machines need to be available to support the CSI Local Support Service

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177

Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request this service please complete the Customer Request Form and contact NCI Agency Demand Management.

https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall CSI availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

CSI functional component	Target Availability	Performance threshold (initial access time)	Remarks
CSI Server Application (CSA)	≥ 99.5%	30"	Administrators should be able to load the CSI Server Application (MSA) within 30 sec.
CSI Console Application (CCA)	≥ 99.5%	20"	User should be able to access CSI Console Application (CCA) within 30 sec.

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 1 hour.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service flavours is listed in the table below. Where the unit of measure is states as n/a, the service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Service/Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP087	CSI Application Service	CSI software maintenance and in service support	n/a

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP087	CSI Application Service	CSI instance installation and in service support	n/a
INF041	CSI Local Support Service	Support delivered to CSI at NCS Units by local Staff (CSUs)	per instantiation

APP088 CINEMA (CSI Integrated Network Monitoring and Management Application) Service

Service ID: APP088

Service Name: CSI Integrated Network Monitoring and Management Application (CINEMA) Service

Portfolio Group: Application Services

Service Description: CINEMA is an operationally proven Link 16 network monitoring and dynamic network management solution.

L16 Network management enables efficient use of the available bandwidth and provides alerts on inadvertent misuse of the frequency spectrum and violation of FCA regulations. Cinema addresses these needs using flexible solution.

The CINEMA runs on standard/COTS Windows PC or Solaris Workstation.

Value proposition: The CINEMA Service provides its users with the following number of key benefits:

- **L16 Network Monitoring**
Enhanced Link 16 network monitoring capabilities sufficient to assure conformity with the nations' Frequency Clearance Agreement (FCA) requirements
- **L16 Dynamic Network Management**
Reconfiguration of platform time slot assignments in real-time in case of over-loaded platform, under-utilised network capacity. Reconfiguring the assignments within the network design assures the intended tactical data information exchange
- **Terminal Monitoring & Control**
Provides a flexible solution that can be set-up to monitor and control of a single-terminal network up to a multi-terminal/multi-network infrastructure with numerous remote MIDS sites.

Service Features: The CINEMA Service is comprised of the following features:

- **Monitor and control L16 ground equipment suites/MIDS terminal(s).**
 - Supports direct (over WAN) connection to the MIDS/STT having the Platform D/J/R interface.
 - Supports terminal discrete control(Power Off/On/Standby)
 - Initialisation, control & monitoring of local and remote terminals
- **Monitor Link 16 Network(s)**
 - Network participation monitoring
 - Time slot monitoring
 - Operational Network Plan and network design compliance monitoring
 - Link-16 messages monitoring
 - Frequency Clearance Agreement (FCA) compliance monitoring

- Guarding against ATC/Nav-aid interference within commercial airspace
- Timeslot utilisation monitoring
- Time slot duty factor (TSDF) monitoring
 - on individual platforms
 - on platform centric areas
 - on user defined areas
 - on a position
- Dynamic network management of networks and platforms
- Free text message(J28.2 and ANFT) capability
- User friendly HMI and Situational Awareness (SA) display
- Recording and reporting

CINEMA Server– Cinema Server is the server-application that establishes connection to the terminals and processes the Link 16 data. The server is running headless.

Cinema Console– Cinema Console is the user interface of the server. One server application can serve multiple console applications. The communication between the server and the console is done via a powerful MongoDB database, which is also used as a storage for the recordings and the Link 16 data.

Service Flavours:

CINEMA software maintenance and in service support: (singleton service provided to Members of the CSI Board) Includes the development, testing, documentation, release of the CINEMA baseline to all sites registered for CSI. However, the sites themselves are responsible for the system update.

CINEMA instance installation and in service support: Upon request, CINEMA instances can be provided through an installation service to customers of the CSI Board. Such services and related support are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

Available on:

NATO Confidential
NATO Secret
Mission Secret

The Service may be available on other networks upon a New Service Request.

Service prerequisites:

NDW002 NATO Digital Workplace Service (High Side)

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)

Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177

Netherlands +31 70 374 3177

Italy +39 081 721 3177

Germany +49 282 4978 3177

USA +1 757 747 3177

For NATO HQ +32 02 707 5858

Service Requests:

To request this service please complete the Customer Request Form and contact NCI Agency Demand Management.

https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall CSI availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

CINEMA functional component	Target Availability	Performance threshold (initial access time)	Remarks
CINEMA Server Application (CSA)	≥ 99.5%	30"	Administrators should be able to load the CINEMA Server Application (CSA) within 30 sec.
CINEMA Console Application (CCA)	≥ 99.5%	20"	User should be able to access CINEMA Console Application (CCA) within 30 sec.

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 1 hour.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.



Service Cost / Price: There is no standard service rate for the service flavours. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

APP091 CSI JREAP Router Application Service

Service ID: APP091

Service Name: CSI JREAP Router Application Service

Portfolio Group: Application Services

Service Description: The JREAP Router is a software-based tactical data link (TDL) solution that enables data forwarding between multiple Link 16 networks over the JRE interface.

The JREAP Router runs on standard/COTS Windows PC or Solaris Workstation, and can either be run as a desktop application (with HMI), or as an operating system service. Software is used for enabling exchange, filtering, and routing (forwarded/relayed) of Link16 j-series messages (i.e. tactical picture) over the Joint Range Extension (JRE) Application Protocol (JREAP) among (near) real-time C2 systems.

With the JREAP Router software, it is possible to connect to a configurable amount of JRE endpoints. A “JRE endpoint” is simply a piece of software, which is located at Command and Control (C2) systems that have access to both Link 16 and alternate communications media (e.g., SATCOM, Fiber Optic, Land Line, or any combination of these or other communications networks).

The tactical picture received from connected JRE endpoint(s) could be forwarded to other JRE endpoint(s). While this forwarding is taking place, it is possible to apply JREAP tactical filters that can be used to reduce the amount of traffic that is being exchanged.

Value proposition: The JREAP Router Application Service provides its users with the following number of key benefits:

- Operate geographically dispersed units.
- Provide reach back to tactical picture from higher/rear C2 nodes/echelons.
- Overcome the requirement to necessarily provide dedicated airborne MIDS/JTIDS relays when their deployment would not be possible.
- Provide Link 16 data communication between surface / ground units when no airborne relays are available.
- Provide backup communications in the event of the loss of the normal link.
- Provide a connection to a platform that may not be equipped with the specialized communications equipment for that TDL.

Service Features: The JREAP Router software offers a configurable amount of channels (32 by default), each of which could be designated to support either of the following communication protocols, so as to support communication over either JREAP Appendix C (TCP/IP), Appendix B (Serial, Synchronous or Asynchronous), Appendix A (Announced Token Passing):

The JREAP-C interface/protocol supported is based on Internet Protocol (IP) (User Datagram Protocol (UDP) Unicast, and Transmission Control Protocol (TCP)).

The JREAP-B interface/protocol supported is based on Full-Duplex Synchronous and Asynchronous Point-to-Point.

The JREAP-A interface/protocol supported is based on Half-Duplex Announced Token Passing.

The JREAP Router receives Link16 data via its channels. The data received, could be filtered, and forwarded/routed within its channels.

The JREAP Router enables the user to visualize the received and/or transmitted picture per channel on a geographical display.

The JREAP Router provides On-line and Off-line data extraction capabilities of all messages exchanged on all channels.

JREAP Router exists in the following configurations:

JREAP Router Standalone – A lightweight self-contained version of the JReapRouter without the need of a database ideal for use on mobile platforms.

JREAP Router Client/Server – A client/server version. The server is running headless and the communication between the server and the client is done via a powerful MongoDB database which is also used as a storage for the tactical data link messages.

Service Flavours:

JREAP Router software maintenance and in service support: (singleton service provided to Members of the CSI Board) Includes the development, testing, documentation and release of the JREAP Router baseline to all sites registered for CSI. However, the sites themselves are responsible for the system update.

JREAP Router installation and in service support: Upon request, JREAP Router instances can be provided through an installation service. Such services and related support are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

Available on:

NATO Restricted
NATO Confidential
NATO Secret
Mission Secret

The Service may be available on other networks upon a New Service Request.

Service prerequisites:

NDW002 NATO Digital Workplace Service (High Side)/ WPS006 REACH Mobile Workplace Service

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177

Netherlands +31 70 374 3177

Italy +39 081 721 3177

Germany +49 282 4978 3177

USA +1 757 747 3177

For NATO HQ +32 02 707 5858

Service Requests:

To request this service please complete the Customer Request Form and contact NCI Agency Demand Management.

https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall CSI availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

JREAP Router functional component	Target Availability	Performance threshold (initial access time)	Remarks
JREAP Router Server Application (JSA)	≥ 99.5%	30"	Administrators should be able to load the JREAP Router Server Application (JSA) within 30 sec.
JREAP Router Console Application (JCA)	≥ 99.5%	20"	User should be able to access JREAP Router Console Application (JCA) within 30 sec.

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 1 hour.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: There is no standard service rate for the service flavours. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

APP092 Ship-Shore-Ship Buffer (SSSB) Application Service

Service ID: APP092

Service Name: Ship-Shore-Ship Buffer (SSSB) Application Service

Portfolio Group: Application Service

Service Description: The Ship-Shore-Ship-Buffer is a flexible, low-cost, state-of-the-art solution to support the communication between Air Defence Ground Systems, Maritime Forces and Airborne Early Warning via Tactical Data Links.

The SSSB system consists of a server and a client application which run on Commercial-Off-The-Shelf (COTS) platforms. The Buffer Operational Server (BOS) is the server application and the SSSB Console (CONS) is the client application. The data connection between server and client application is extremely efficient and allow the use of the client in local and remote mode using low bandwidth communication lines without any degradation of the user experience.

The SSSB server and client applications implement a sophisticated scripting language which allows full automation of user operations and training scenarios. Additionally the synchronization scripting commands and the support of distributed architectures allows the SSSB server and client applications to be used for TDL training and TDL testing.

The SSSB Server and client applications have been developed completely using the JAVA programming language to allow not only to support all the available hardware and software platforms but also to achieve a very short time in implementing enhancement and corrections as required by the SSSB user's community.

Part of the SSSB System products there is the Open-System-Communication-Control (OSCC) system which provides full control of communication equipment. OSCC is a client/server application which runs on COTS platforms. OSCC support already more than 50 communication equipment which range from radios (transmitters, receivers and transceivers), matrices (antenna, analogue and digital audio), Data Terminal Sets (DTS), discrete signals etc. Additional equipment can be added also by third parties using the OSCC Software Development Kit (SDK).

OSCC, for its distributed design, can support local and remote connections, full or limited access to equipment parameters from users with different authorization rights.

OSCC integrates VoIP/RoIP functions for voice coordination and to connect to military and civilian telephone networks.

The NCI Agency has developed specific Diagnostic Tools to assist the troubleshooting of TDL communication problems. The SSSB Diagnostic Tools can be used either by site personnel or by NCI Agency personnel when in depth troubleshooting is required.

The NCI Agency's AMDC2 offers a number of services for utilizing and supporting SSSB in operational and training environments and provides other services related to SSSB such as Management and Engineering support. A high level overview of offered services for SSSB is

presented within the following chapters, a detailed description is provided in the SSSB MOU document.

Value proposition: The software products of the SSSB family provide a complete and integrated set of state of the art applications that enable the users to apply full control of:

- Tactical Data Link channel resources;
- Tactical Data Link Networks management;
- Voice coordination channels and;
- Communication equipment control and monitoring.

The technology insertions developed by the NCI Agency for the SSSB System has resulted in the definition of a new architecture for the deployment of the NATO SSSB Modernization Project based on IP interfaces to allow a flexible use of local and remote resource among all NATO SSSB installations.

SSSB provides a migration path from Link 11 to Link 22 supporting mixed Link 11/22 environment. The migration support covers all the Link 22 aspects from TDL messages, Network management, radio resources, TDL interoperability, communication monitor and troubleshooting.

Service Features: To assist the SSSB users in gaining and maintaining the Tactical Data Links communication the following areas are supported:

- Tactical Data Link formats: Link 1, Link 11, Link 11B, Link 22, JReaP;
- Non-Tactical Data Link formats: AIS (Automatic Identification System);
- Tactical Data Link transports: SIMPLE;
- Maintaining and exchanging of a real-time Recognised Air, Surface and Subsurface Picture (RASSP) based on TDL and non-TDL inputs;
- Controlling and monitoring Link 11 and Link 22 TDL Networks;
- Controlling and monitoring local and remote communication equipment associated to the TDL channels: Antennas, Radios, Switching Boxes, Modems, and Multiplexers etc.;
- Diagnosis of TLD communication infrastructure.

Service Flavours: SSSB is provided as a singleton service to the members or the SSSB Board. This singleton service includes:

- System Engineering support,
- Post design services,
- Documentation,
- Project management,
- Training support,
- Configuration management,
- Troubleshooting for communication,
- Maintenance and supply support,
- Transportation,
- Procurement and
- Quality and safety assurance.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

SSSB relies on an infrastructure able to host SSSB applications and enabling intra and inter-site data exchange through networking services.

PLT013 – NATO Integrated Secure Platform can be utilised to run SSSB application on a secured Solaris or Oracle Linux platform as required.

Serial Link 1 connections require that inter CRC infrastructure exists allowing the transport of serial data. SSSB support dedicated serial lines and virtual serial lines over network connections.

Link 11 connections require local and/or remote HF/UHF radio infrastructure, Data Terminal Set modem and Link 11 cryptographic equipment. SSSB provides direct support of all existing format of DTS models and interfaces as well as Link 11 cryptographic equipment. SSSB support both dedicated and IP communication for remote Link 11 infrastructures.

Serial Link 11B connections require secure connections with the remote systems. SSSB supports dedicated serial lines and virtual serial lines over network connections.

AIS connections require either a dedicated receiver or a connection to a National AIS concentrator facility. In the latter case, due to the different security levels, it is mandatory the use a serial diode between the systems.

SIMPLE connections require secure lines. Generally the SSSB SIMPLE ports are connected to the CFBLNet or NATO WAN networks.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Ops Centre personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

- Belgium +32 65 44 3177
- Netherlands +31 70 374 3177

- Italy +39 081 721 3177
- Germany +49 282 4978 3177
- USA +1 757 747 3177
- For NATO HQ +32 02 707 5858

Service Requests:

To request the SSSB Application service or related information, please complete the Customer Request Form and contact NCI Agency through the submit function included in the form following the link below.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The support provided by the NCI Agency for the SSSB system covers so many areas that a list of all the applicable key metrics will not provide any additional value. The Key Metric that can summarize all of them is the one that measure the grade of implementation of the Program of Work (PoW), as agreed by the Participants to the SSSB MOU.

Table 1: SSSB PoW Implementation

Indicator	PoW Implementation
Description	This indicator measure the level of implementation of the PoW activities agreed the SSSB Board (Participants to the SSSB MOU). The PoW is a mixed set of Common Activities, like Software Maintenance, and Had Hoc Activities.
Measurement Method	Measuring the percentage of implementation of PoW activities.
Unit	%
Algorithm	Difference between actual and estimated man power
Target	Metric $\geq$ 85%
Applicability	All PoW entries

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.



Service Cost / Price: There is no standard service rate for this service. The total of the Service delivery cost is charged in accordance with the POW developed and agreed with the SSSB Board.

APP093 Enterprise Architect Application Service

Service ID: APP093

Service Name: Enterprise Architect Application Service

Service Type: Customer Facing

Portfolio Group: Application Services

Service Status: Pipeline

Service Description:

Service is based on the application Enterprise Architect (EA), which is a visual modelling and design tool based on UML. EA supports:

- the design and construction of software systems;
- modelling business processes;
- modelling industry based domains.

It can be used not only to model the architecture of systems, but to process the implementation of these models across the full application development life-cycle.

Systems modelling using UML provides a basis for modelling all aspects of organizational architecture, along with the ability to provide a foundation for designing and implementing new systems or changing existing systems. The aspects that can be covered by this type of modelling range from laying out organizational or systems architectures, business process reengineering, business analysis, and service-oriented architectures and web modelling, through to application and database design and re-engineering, and development of embedded systems.

Value Proposition:

Provisioning of Enterprise Architect application as a service supports complete system/application lifecycle management, starting from requirements modelling down to physical components, artefacts and infrastructure, while enabling architects/designers/analysts and software developers to benefit from a complete traceability between each model. Out of the box, EA has support for industry leading standards for system analysis and design (Unified Modelling Language - UML), business process analysis (Business Process Modelling Notation – BPMN, Decision Modelling Notation – DMN) as well as enterprise architecture modelling (ArchiMate 3.0.1, TOGAF). Many other standards are supported out of the box (ArcGIS, Iconix, SoMF, SysML and others).

Enterprise Architect supports architecture development using NATO Architecture Framework (NAF v4), with a free MDG plugin for Enterprise Architect. It also includes document templates for Business Analysts (based on Business Analysis Body of Knowledge – BABOK), Business Architects (based on Business Architects Guild's BIZBOK). Additionally, it includes design-to-code with code generation from model, and data base entities generation from the model.

Service Flavours and Features:

1. APP093-1 Enterprise Architect – provision of a validated standalone software deployable on authorized networks, enabled for a single user, without collaboration

features like access to a shared network database repository. It is installed directly on an end-user terminal;

2. APP093-2 Collaboration Repository – provision of a collaboration repository, hosted on central infrastructure, enabled for an access to a shared network database repository, requires holding a valid Enterprise Architect (Flavour 1). This option enables true collaboration for a team of experts, knowledge sharing and exchange, discussions and shared project planning/execution.
3. APP093-3 ProCloud and Prolaborate Integrations - Prolaborate allows users to create tailored set of views that reduce complexity, focus attention and increase the accessibility of model information for the non-modelling community who are more concerned with consuming the models. Prolaborate also provides dashboards, impact analysis, gated reviews and much more to leverage information from the model to provide unique windows into the model for a custom audience.
4. APP093-4 Training package - Tailor and preparation of material, includes meetings with the customer to capture the scope up to 10 hours.

Activities in scope of service:

- Service management of entire service lifecycle including regular user communication;
- Requirements analysis and validation with the customer:
 - o Propose technical solution;
 - o Evaluate and propose costs based on requirements and technical solution;
- Application management:
 - o Incident Management:
 - Issue Investigation and Resolution; Escalation of tickets to 3rd party supplier when required and follow up until their final resolution;
 - o Independent Verification & Validation:
 - Change Configuration Proposal (CCP) Submission and Follow up;
 - o Deployment:
 - Configuration & Reconfiguration;
 - Deploying & Release, and Patches Management;
 - o Operations:
 - Operate and perform the required maintenance on the application servers and the underlying platform;
 - Set up and Maintenance required Reference/Test and Development environment in NSF and make it available for the customer.

Available on:

- NATO Unclassified
- NATO Restricted
- NATO Secret
- Mission Secret

The service may be available, on request, on other security domains.

Service Prerequisites:

- NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)/ WPS006 REACH Mobile Workplace Service
- WPS002 User Access Services

Standard Service Support Levels: N/A

Service Availability Target: 99.5% Yearly Availability for flavour 2 and 3, which have backend services

Service Restoration: For collaborative versions using repository only – service restoration within SLA boundaries.

Service Cost / Price: The cost is calculated per Flavour per number of users, number of repositories (costing model still under development, to request this service a CRF is required in order to obtain a price proposal).

APP095 Agile Tools for task management - JIRA Software Service

Service ID: APP095

Service Name: Agile Tools for task management - JIRA Software Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Pipeline

Service Description:

JIRA is a family of software products that various types of teams can use to manage issues and tasks and handle daily team work, activities and objectives.

JIRA Software (JS) is the product based on Agile methodology that can be used for planning, tracking and reporting internal team activities. Teams and team managers can use the included boards for task management based on Agile methodology. Additionally Jira Software can be used for task management, software development, software testing, bug tracking, Agile project management, scrum management. Team productivity can be monitored using the included time tracking capabilities. Real time reports on progress are available.

JIRA Service Management (JSM) is the product used for ticket and request management that enable teams of agents to be in contact with customers and solve various non-it, business types of requests. Jira Service Management provides any service team the capabilities to be in contact with the customer and answer customer's requests according with procedures and SLAs in place. Team productivity can be monitored using the included KPIs and time tracking capabilities. Real time reports on status progress are available.

Confluence is the knowledge base product that can be integrated with both Jira Software and Jira Service Management. It can be used:

- with JIRA Software, to improve the documentation and information available to team members;
- with JIRA Service Management, to provide a self-service place to find answers before asking questions.

Value Proposition:

The service offers customer:

- by using JS accessing Scrum and Kanban boards out-of-the box (boards are task management hubs, where tasks are mapped to customizable workflows);
- by using JS, boards provide transparency across teamwork and visibility into the status of every work item;
- by using JS, boards can be used as activity lists for the team or team members;
- by using JSM tracking of activities inside teams if a process requires multiple team members to interact or it takes a long time to complete;
- by using JSM the possibility for a customer of a service team to make non-it requests to that service team and track request status until is resolved (requests are mapped to customizable workflows);
- by using Confluence, a knowledge base can be built and it can contain information related to processes, procedures, workflows, documents;

- by using Confluence integrated with JSM a knowledge portal with most common problems, procedures and solutions can be implemented;
- by using Confluence integrated with JS the activities and tasks inside JS can be documented;
- team productivity can be monitored using the included KPIs (for JSM), time tracking capabilities (for both JS and JSM) and real time performance reports with sprint reports and velocity charts (for JS).

Service Flavours and Features: Service is available as one of the 3 flavours below and in each case this consists of the base software and the add-ons as listed for each of the base software. Flavours can also be combined, depending on the request.

1. JIRA Software, including the add-ons:
 - Zephyr Scale – Test Management for JIRA Data Center
 - Configuration Manager for Jira (CMJ) Data Center
 - R4J – Requirements Management for Jira Data Center
 - Xporter – Export issues from Jira Data Center
2. JIRA Service Management, including the add-ons:
 - Kanban Boards for Jira Service Management
 - Refined for Jira
3. Confluence - Can be used as a standalone deployment or integrated with JIRA Software or JIRA Service Management;
4. Training

Activities in scope of service:

- Service management of entire service lifecycle including regular user communication;
- Requirements analysis and validation with the customer:
 - o Propose technical solution;
 - o Evaluate and propose costs based on requirements and technical solution;
- Application management:
 - o Incident Management:
 - Issue Investigation and Resolution; Escalation of tickets to 3rd party supplier when required and follow up until their final resolution;
 - o Independent Verification & Validation:
 - Change Configuration Proposal (CCP) Submission and Follow up;
 - o Deployment:
 - Configuration & Reconfiguration;
 - Deploying & Release, and Patches Management;
 - o Operations:
 - Operate and perform the required maintenance on the application servers and the underlying platform;
 - Set up and Maintenance required Reference/Test and Development environment in NSF and make it available for the customer.

Available on:

- NATO Unclassified

- NATO Restricted
- NATO Secret

The service may be available, on request, on other security domains.

Service Prerequisites:

- NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)/ WPS006 REACH Mobile Workplace Service
- WPS002 User Access Services

Standard Service Support Levels:

Service Availability Target: 99.5% Yearly Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period is 8 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the relevant NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery (costing model still under development, to request this service a CRF is required in order to obtain a price proposal).

APP100 Mobile Advisor Reporting Tool (MART)

Service ID: APP100

Service Name: Mobile Advisor Reporting Tool (MART)

Service Type: Customer Facing

Portfolio Group: Application Services

Service Status: Available

Service Description: The Mobile Advisor Reporting Tool (MART) enables Civil-Military Cooperation (CIMIC) / J9 staff to capture and record the outcomes of their engagements in the field. Through a modern, simple and user-friendly Internet accessible web application, end-users can draft, save and submit their engagement reports that will be delivered to the Advisor Network (ANET) database. Reports can be sent over data diodes, so they can reach the high side HQ operational network, not connected to the Internet.

Value Proposition: Accessible via any mobile device, this cloud-based application provides end-users with the capability of submitting engagement reports from anywhere and right after the engagement has taken place. Once the reports are processed and stored in the ANET database, they are deleted from the cloud storage to ensure confidentiality of the collected information.

Service Features:

MART comprises the following features:

- Draft, save, print, export (as PDF), and submit engagement reports
- Cloud-based front-end application reachable from any internet enabled Mobile Device
- Tailored report template including lookup tables and free-text fields
- Storing of submitted reports in the Advisor Network database
- Report Attachments
- Supports for external authentication services, such as, but not limited to, AWS Cognito, OpenID Connect, SAML, Active Directory Federation Services

Service Ordering and Request: Customer Request Form

Service Flavours: The Service is available in 3 flavours, based on the number of users:

1. APP100-1 Small deployment: 0-200 users
2. APP100-2 Medium deployment: 200-2,000 users
3. APP100-3 Large deployment: 2,000-10,000 users

Available on: Public accessible Internet services, limited to NATO UNCLASSIFIED content

Service Prerequisites:

APP068 – Advisor Network Application Service

Standard Service Support Levels:

Service Availability¹ Target: 99.0% Availability

Service Restoration:

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes



Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting: Standardised service reporting to customers in accordance with the NCI Agency SLAs

Available NCI Academy Training not covered by service cost: N/A

Service Cost / Price: The unit of measure for the service is Per Deployment. Price details available in the Service Rates Document.

APP102 – REACT – PNT and NAVWAR Application Service

Service ID: APP102

Service Name: REACT – PNT and NAVWAR Application Service

Portfolio Group: Application Services

Service Description: The REACT – Positioning Navigation and Timing and Navigation Warfare Application Service is based on the Navigation Warfare functionalities of the NATO Software REACT (Radar, Electronic warfare and Communications coverage Tool). It provides the operational user with an intuitive way to develop Navigation Warfare (NAVWAR) products allowing decision makers to increase their situational awareness during planning and execution of air, ground or maritime operations. The operational user can generate predictions of Global Navigation Satellite System (GNSS) jamming effects within an area of interest based on specific GNSS jammer parameters and propagation models. The REACT tool can be hosted within the NATO Command Structure's Bi-Strategic Command (Bi-SC) Automated Information System (AIS) or hosted on a standalone local instance or internet-facing computer.

Value Proposition: REACT provides the NATO Navigation, Electromagnetic Operations Warfare and Space Communities with a capability that enables the following operational benefits:

- Support the Intelligence and other relevant Communities in visualising and understanding the effects of collected data from NAVWAR jamming systems.
- Sharing of intelligence services and data across NATO at all command levels.
- Enhance the dissemination of intelligence with Nations and other domains.
- Increased support to situational awareness, common operational picture, and mission planning and execution.
- Support to all operational mission types.
- Unique analytics and propagation modelling capability not available in other NATO systems.
- Support exercises and training activities within the NAVWAR, EMO and Space Communities.

Service Features: The REACT – PNT and NAVWAR Application Service is comprised of the following modules and features:

- Front-end: a user-friendly Web application with services interacting with the REACT Tool back-end server modules
- Back-end: a calculation module comprising of several advanced analytical models that returns results to the REACT Web client or other NATO FAS clients using the WMS data exchange format.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
NATO Partner network (For NNHQ)

Service prerequisites:

APP055 - Core GIS Geospatial Services (pre-required if no WMS compatible mapping provision service is available)

Standard Service support levels:

Service Availability¹ Target: 99.5% Availability

Service Restoration: for NCS customers, the restoration priority will be as specified in centralised or local service level agreement.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Service transitioned to NDW006.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP104 Medical Management Application Service

Service ID: APP104

Service Name: Medical Management Application Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Available

Service Description: Medical Management Application Service facilitates theatre medical staff in conducting Patient Tracking, Patient Regulating, Medical Capability Directory and Medical Reporting functions. The Medical Management application Service also enables the applicable contribution to Recognized Medical Picture to support Commander's decision making process.

Value Proposition: The Medical Management Application Service save lives through rapid decision making; medical management information is digitized empowering staff to make timely decisions based upon current situation information.

Service Features: The Medical Management Application Service provides minimum military functionality for the following medical functions:

- Medical Capability Directory,
- Patient Tracking,
- Patient Regulating,
- Medical Reporting
- Recognized Medical Picture.

Service Request: CRF can be raised for new request.

Service Flavours:

1. APP104-1 Product Lifecycle Support

Product Lifecycle Support service includes the activities to provide centralized baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management and service delivery management during one year.

The cost drivers for product lifecycle support services are described below.

- **Service Delivery Management** – Service Delivery management is responsible for the day-to-day operations of the medical functional services and ensures the smooth delivery of IT services to customers and end-users. Service delivery focus is on the operations, quality, and improvement of services throughout their lifecycle within agreed levels of service.
- **Maintenance** – Medical Management Application Maintenance is subject to Change Management Governance by Change Control Board (CCB), led by SHAPE J6/JMED. Typically, one major and one minor release is planned each year. All new versions are backward compatible.
- **Release Management** – The release management includes the efforts to package, build, test and release the new Medical Management Application versions. Releases undergo various testing processes to ensure that the product is interoperable, fit for purpose and use, and ready to be made available. These activities are performed by various NCIA teams as well as user communities, ranging from functional SMEs to security experts.
- **Reference Data Management** – Management of underlying reference data such as nations (including artificial exercise nations), medical capabilities and speciality care.
- **Distribution and NATO Software Resource Management** – Medical Management Application Service products are available the Electronic Definitive Media Library (EDML) download portal.

2. APP104-2 Instance (APP104-2)

This flavour provides for a single running copy (instance) of an application on specified network domain with its own specific setup, configuration and user access. This includes the maintenance and support for the running instance, such as OS upgrades and application upgrades, hot-fixes, and backup and recovery management. It does not include underlying costs of hosting infrastructure and platform of the instance. The cost drivers include:

- **Enterprise Change Management Governance;**
- **Operational infrastructure and platform costs specific to the service;**
- **1st Level Support** – This is the initial point of contact for user inquiries, technical issues, and disruptions;
- **2nd Level Support** – This service is provided by C2BA Centralised Level 2 Support. It includes fixing configuration issues, troubleshooting, deployment of upgrades and hot-fixes.
- **3rd Level Support** – This service is provided by C2BA and contractors. It provides the highest level of specialist skills available in order to fulfil support requests.

3. APP104-3 User Support

This flavour offers user access management and user support for all levels of users. The flavour applies to one site for a defined number of users with applicable sizes listed in Table 1. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year. The cost drivers include:

- **1st Level Support** – This is the initial point of contact for user inquiries, technical issues, and disruptions;
- **2nd Level Support** – This service is provided by C2BA Centralised Level 2 Support. It includes fixing configuration issues, troubleshooting, and access management. This service is provided via an operational level agreement with the C2BA Centralised Level 2 Support team and costed as such;
- **3rd Level Support** – This service is provided by C2BA and contractors. It provides the highest level of specialist skills available in order to fulfil support requests.

Table 1 User Support sizes

User Support sizes	Number of users
APP104-3A User Support Small	Up to 50
APP104-3B User Support Medium	Between 50 and 250
APP104-3C User Support Large	Above 250

4. APP104-4 New Instance / Service support

This flavour offers implementation of a new instance on any supported security domain. The cost includes: the feasibility study, one requirement workshop at customer premises, installation and configuration and initial knowledge transfer.

Available on:

- Any network of customer,
- NATO Secret,
- Mission Secret, VeVA,
- NATO Unclassified.

Service Prerequisites: NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)

Standard Service Support Levels:

Service Availability¹ Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The cost of service is composed of a product life cycle support cost which is a necessary cost to keep the product running regardless of the number of sites running the application, the product lifecycle support unit of measure is unit 1. There is also a cost for deployment and support flavours depending on the size of the site, the unit of measure for these flavours is per site. The cost details are listed in the service rate section of this catalogue release.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP105 Exercise Portal Template Set (EXPOTS)

Service ID: APP105

Service Name: Exercise Portal Template Set (EXPOTS)

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: *Available*

Service Description: The Exercise Portal Template Set provides a configurable set of Sharepoint templates to manage an exercise programme including exercises that are part of a recurring series. Specific exercise portals can be instantiated that have a structure that reflects the latest Bi-SC 75-3 exercise process stages. It also provides scenario setting templates and lessons learned templates from which specific portals can be instantiated rapidly to meet the needs of specific exercise communities. The initial user community is the Ballistic Missile Defence (BMD).

Value Proposition: This service aims at providing an exercise programming portal from which default exercise portals can be generated. In addition a pre-defined set of Sharepoint portal templates from which specific portals or sub-portals can be instantiated to support the management of setting information or the management of lessons learned. These templates can be applied to extend exercise portals or a stand-alone portals. Sharepoint users with appropriate rights can subsequently customise the portals. For each type of portal template a standard set of user roles is included that specifies the associated privileges. By assigning users to Sharepoint groups, their privileges can be set per portal type.

Service Features:

- Exercise programming and scheduling portal with viewer, contributor and manager roles. Adopts the structure of the Military Training and Exercise Programme (MTEP) in order to facilitate the export of data to the MTEP-supporting application. Exercises can be marked as being part of a recurring series to support BMD requirements. An exercise portal can be instantiated for a single exercise or for a recurring set.
- Instantiated exercise portals are structured according to the stages of exercise planning endorsed by SHAPE in September 2023.
- Exercise setting and scenario template with setting builder and setting viewer user groups. The exercise setting and scenario template can be used to instantiate an actual portal according to the setting and scenario data structure defined in the Bi-SC 73-3. In addition, a number of BMD-specific sections are added to the structure.
- Exercise Lessons Management portal template that implements a workflow that corresponds to the lessons learned process specified in the latest Bi-SC Directive 080-006. The templates support the collection of observations, the grouping of observations into lessons identified or best practices, the management of remedial action and associated plans. For specific exercises, an offline observation capturing form can be generated and imported. A combined view of the various lessons information items is available. An extensive search capability is included to query the content. Portal user groups are defined for viewers, contributors, lessons managers, tasking managers, action managers, local managers and portal managers.

Service Ordering and Request: For NCS users, the service can be requested through service legal agreements or through the In Service Support programmes of work for Air C2-related work.

Service Flavours: The portals templates and instances can be requested separately.

Available on: NS and PAN

Service Prerequisites: Sharepoint PLT003

Standard Service Support Levels:

Service Availability¹ Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.]

Service Reporting: According to relevant SLA reporting.

Available NCI Academy Training not covered by service cost: None

Service Cost / Price: The service cost will be charged for each instance of the service deployed to a specific server.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP110 Information Environment Assessment (IEA)

Service Name: Information Environment Assessment

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Pipeline

Service Description: The IEA service provides to NATO consumers of Publicly Available Information (PAI) an integrated data-sourcing and analytics platform to collect and understand the Information Environment (IE).

Value Proposition: The IEA service provides the following value and benefits:

- Consolidated data access: the IEA service provides a hub for PAI, aggregating data collected through commercial subscriptions, Internet scraping, audience research, and ad-hoc PAI sources. The IEA service allows the data to be filtered to focus on NATO's topics of interest.
- Advanced data analytics: the IEA services leverages the latest data analytics methods, generative AI, entity extraction to expose data to the NATO analyst in the form of interactive dashboards and visualizations to support collection and data exploitation.
- System environment: the IEA service provides a NATO-hosted collaborative environment allowing the PAI-consuming operators to organize and plan their collections, create and store bundles of processed data for archival, further retrieval and processing, and use advanced hosted analytics on NATO internal data.

Service Features:

- Commercial subscriptions: provides the ability to connect to existing data sources, or to trigger the procurement of additional ones to meet domain-specific requirements.
- Internet scrapers: provides the ability to collect specific data directly on the surface web, and selected areas of the deep web and dark web.
- Data-science and collaboration platform: provides the ability to search, transform, share and present data.
- Data-science support: provides the ability to get data-science and AI subject matter experts integrate ad-hoc data sources, develop advanced visualizations or provide consultancy on to PAI communities of interest.

Service Request:

- Access to the IEA service based on existing service features (data-sources, analytics) will be requested through ITSM service requests on a per-user account basis.
- Requests for additional service features will be managed through a data change process, in order to capture community-specific requirements, the procurement strategy, and funding.

Service Flavours:

1. IEA system environment management: the NCIA service delivery manager will provide the 2nd level support to the IEA platform, manage service requests and incidents, and collect continued improvement feedback and data requirements.
2. IEA data-services contracts management: the NCIA contracting officer and the NCIA service delivery manager acting at the Contracting Officer Technical Representative (COTR) will manage the performance of the existing data-services contracts and validate the service level agreement metrics.
3. IEA data-services contracting: the NCIA contracting officer and the NCIA service area owner will organize the procurement of additional data services or the renewal of the existing ones, based on the NATO acquisition procurement regulations. This process can have a variable time range depending on the magnitude and complexity of the services requirements.
4. IEA data-science support: the NCIA data-scientist and operational analyst will support the service users to optimize the use of their data, incorporate ad-hoc data-sources and analytics into the IEA platform, support recruitment and training of analysts in the NATO Enterprise.

Available on:

- NATO UNCLASSIFIED
- NATO-operated Azure public cloud & commercial Internet platforms

Service Prerequisites:

- The IEA service users will need Microsoft Online accounts to access the IEA system environment.
- The IEA service users will need contractor-specific accounts to access the IEA analytics platform.
- The IEA service users can optionally subscribe to the Enterprise Internet Service [INF003], service flavor Anonymized Browsing, in order to meet the non-attributable identity requirements for the service.
- The IEA platform requires the Cloud Services Management and Integration (CSMI) Service [PLT010] for the hosting, security and operations of the IEA platform.

Standard Service Support Levels:

Service Availability¹ Target: the service availability target is negotiated on a per-data-service basis. The target for the data-services contract is 98% during business hours (Mon-Fri 08.00-18.00 CET), meaning a maximum of 1 hour downtime per week on a quarterly average.

Service Restoration: the service restoration target is 2h during business hours (Mon-Fri 08.00-18.00 CET) and 12h outside business hours.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: $\frac{(\text{Available Minutes}^* - \text{Downtime})}{\text{Available Minutes}} \times 100$

*Minutes available during agreed reporting period excluding planned maintenance minutes

APP113 Operational Application Support Service

Service Name: Operational Application Support Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Available

Service Description:

Operational Application Support Service maintains and supports a consistent and interoperable FAS set up for External Customers and stakeholders. It provides technical support for external CIS units using the NATO FAS's limited to:

- JCHAT, MLINK, OPENFIRE, JOCWATCH, LOGFAS, TOPFAS, JEMM
- NIRIS (with NISP), ICC, JTS/FAST, SEW, MCCIS
- NCOP, LC2IS, AIRC2IS
- INTEL-FS, HMART, NAMIS, CORE GIS

Service features encompass also the support to NFS and Nations to federate their hosted Application services with NATO Centralized Application services; providing support for federation authorization, NATO services configuration and troubleshooting, as well as management of incidents on NATO site of federated services.

Application services federated on Customer site could be any NATO applications from the list above, or any National applications tested and compliant with FMN approved baseline.

Value Proposition:

This service ensures External Customers' operational support requirements are addressed for the effective use of NATO FASes to enable their preparedness for missions.

The service also enables initialization of and ensures continuity of the Application Services federation between NATO Command Structure and NFS, Nations.

Service Features:

- Support for trouble tickets and service requests[1]
- Monitoring and Event management (if agreed with a Customer and remote access is possible)
- Problem management
- Software upgrades in line with the NCIA approved FAS (COI) baseline as per A2SL (Agency Authorized Software List). It includes:
 - Up to one onsite supported upgrade
 - Up to two remotely supported upgrades of the existing installed FAS (COI) instances (e.g. through emails, ITSM, remote access, and phone)

- Support for federation of services:
 - Configuration of centralized NATO Application services given the requester has authorization from SHAPE or the corresponding Service / Data Owner within NCS
 - Incident management of existing configurations on centralized NATO Application services
 - Application services monitoring & event related corrective actions for agreed set of NATO Enterprise federated application services

By default, the on-site installation is limited to one service instance per FAS (COI) application. Additional instances are subject to resource availability (work force, time, funds).

The scope is a subject to annual refinement, as new applications and versions integrate into NATO FAS (COI) baseline, or old applications become obsolete and out of support.

Change requests to the application deliverables that trigger source code modification are not part of this Service.

[1] In the case NCIA has no remote access (connectivity) to the FAS application services supported, NCIA will provide remote support in the form of guidance in troubleshooting and resolution. Guidance for resolution will include a proposed solution.

Service Ordering and Request:

NCIA Standard Process

Service Flavours:

1. **Bundle B** - Support to JCHAT, MLINK, OPENFIRE, JOCWATCH, LOGFAS, TOPFAS, JEMM
2. **Bundle C** - Support to NIRIS (with NISP), ICC, JTS/FAST, SEW and MCCIS
3. **Bundle D** - Support to NCOP, LC2IS, AIRC2IS
4. **Bundle E** - Support to INTEL-FS, HMART, NAMIS, CORE GIS

Following options can be requested additionally:

On-site Support Option– Available for each bundle, service cost table depicts the additional cost per each bundle.

Federation Add On – Available for each bundle, service cost table depicts the additional cost per each bundle for support to application services federation.

Complete Solution – Includes remote and on-site support for all listed applications (all bundles)

Complete Federated Solution – Includes remote and on-site support for all listed applications (all bundles) including federation support per each bundle.

Tailored (Reduced) FAS (COI) OPS: The Service conditions adopted to meet specific customer requirements (e.g. changed or reduced number of supported applications or adjusted scope of support) per site, per bundle.

Extended FAS (COI) OPS: Support required outside of normal business hours per site, per bundle, on weekends and public holidays; additional charges apply.

Available On:

- Any network of customer subject to security requirements
- NS
- MS

Service Prerequisites:

Minimum of one functional FAS (COI) application on the site requiring the Service.

In case of federated solution;

- Existing network connectivity and Federated Core services (DNS as minimum) between NATO centralized networks (NS and/or MS) and Customers target network.

Standard Service Support Levels:

Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCIA standardised SLA and SSPs with respective customers.

Service Reporting:

See CCSC - Service & Product Attributes e.g. Support Hours, incident/problem reporting.

Available NCI Academy Training not covered by service cost: N/A

Service Cost / Price:

For the flavours/options where there is a defined unit of measure, a standard service cost is specified and the unit of measure and price details for each of the service flavours is specified in the Costed Customer Service Catalogue. For the Extended FAS (COI) OPS and Tailored FAS (COI) OPS Reduced Scale options, the unit of measure is 1, the total of the service delivery cost for these flavours is charged in accordance with specifically arranged conditions of the service delivery.

Service Flavours* / Service Options	Service Unit
Regular FAS OPS - Bundle B	Per Site
Regular FAS OPS - Bundle C	Per Site
Regular FAS OPS - Bundle D	Per Site
Regular FAS OPS - Bundle E	Per Site
Regular FAS OPS - On-Site Support Option	Per Site/Per Bundle
Regular FAS OPS – Federation Add On	Per Site/Per Bundle
Regular FAS OPS – Complete Solution	Per Site
Regular FAS OPS - Complete Federated Solution	Per Site
Tailored (Reduced) FAS OPS	1 (custom calculated)
Extended FAS OPS	1 (custom calculated)

** This service is available only to External NCIA Customers in support of their CIS Support Element*

APP114 Message Text Format Application Service

Service ID: APP114

Service Name: Message Text Format (MTF) Application Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Description: The MTF Service provides a set of information management tools required for the development, format validation and management of Formatted Structured Messages. It is based on COTS products that provides automated support to develop, refine, and manage proposed additions and modifications to the Message Text Formats. It features a repository for newly agreed ADatP-3 formats awaiting publication in new baselines and the developmental components that support message creation. Formats that have been “baselined” and published in the ADatP-3 standard are also retained in a separate area.

Value Proposition:

1. Enables Message Text Format Capability Team/CIS Panel/NATO C3 Board and Information Exchange Harmonization Working Group (IERHWG)/NATO Standardization Office (NSO) to work together to generate STANAG 7149 – NATO MESSAGE CATALOGUE, APP-11.
2. Supports the lifecycle management of MTFs in support of Air, Land, Maritime domains besides several communities such as Medical, CBRN, Joint ISR, and Logistics.
3. Provides a single repository per security domain for all MTF related Configuration Items.
4. Ensures consistent and timely information availability to Stakeholders.
5. Enables easy review, reporting, and validation of information.

Service Features: This service features a set of information management tools, supporting the configuration management and collaboration of the interoperability standardisation community in the development of NATO message text formatted (MTF) standards and standardisation process. The MTF service includes an IRIS Standards Management (ISM) license for up-to 75 users. Note: the information and content management, and application level user access control are customer responsibility.

Service Ordering and Request: This service can be requested via a Customer Request Form.

Service Flavours:

- APP114-1 MTF Product Lifecycle Support: This flavour covers the product lifecycle aspects focussing on the continued support functions required to ensure the readiness and operational availability of the specified application. This includes the activities to provide centralized service portfolio management, baseline maintenance, change and knowledge management, continuous service improvement, release and distribution management, license management and service delivery management during one year.

- APP114-2 MTF Instance: This flavour provides for a single running copy (instance) of an application on specified network domain with its own specific setup, configuration and user access. This includes the hosting infrastructure and platform of the instance on specified network domain, the maintenance and support for the infrastructure, platform and running instance, such as OS upgrades and application upgrades and hot-fixes, and backup and recovery management.
- APP114-3 MTF User Support Small: This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 75 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.
- APP114-4 MTF User Support Medium: This flavour offers user access management and user support for all levels of users. The flavour applies to one site for up to 200 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.
- APP114-5 MTF User Support Large: This flavour offers user access management and user support for all levels of users. The flavour applies to one site with more than 200 users. The flavour includes provision of centralized technical support, incident management, request fulfilment, access management, and problem management during one year.

Available on:

NATO Unclassified

NATO Restricted

NATO Secret

Service Prerequisites:

NDW001 NATO Digital Workplace Service (Low Side) / NDW002 NATO Digital Workplace Service (High Side)/ WPS006 REACH Mobile Workplace Service

INF003 – Enterprise Internet Access Service (only for NATO Unclassified instances of the service)

Standard Service Support Levels:

Service Availability¹ Target: 99 %

Service Restoration: P4 - Restore Target Time: 3 (three) working days

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost: N/A

Service Cost / Price: The cost of this service is composed of a product lifecycle support cost which is a necessary cost to keep the product running regardless of the number of sites

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

running the application. The product lifecycle support unit of measure is unit 1 and includes a bundle of 75 user license; any request for additional user license will have an impact on the product lifecycle cost. There is also a cost for deployment and support flavours depending on the size of the site, the unit of measure for these flavours is per instance and per site respectively. The cost details are listed in the service rate section of this catalogue release.

APP115 Joint Automated Deep Operations Coordination System

Service ID: APP115

Service Name: Joint Automated Deep Operations Coordination System

Service Type: Customer Facing

Portfolio Group: Application Services

Service Status: Pipeline

Service Description: Joint Automated Deep Operations Coordination System (JADOCS) is a Joint and Coalition targeting, coordination mission management software application. It links Command and Control (C2), Intelligence, and Air operations information with execution systems using real time collaborative targeting managers, customized for each service or specific functional area. It is also capable of digitally processing fire missions, as well as generating and sharing targeting data, Fire Support Coordination Measures (FSCM), and Airspace Control Measures (ACM).

Value Proposition: JADOCS is used to significantly enhance the Joint Force and Component Command's capability to simultaneously develop, coordinate and execute Dynamic and Time Sensitive targets and fire missions, as well as battle space coordination, search and rescue, and disaster relief/recover operations worldwide. JADOCS provides coordination and deconfliction of targeting information at all levels of command structure for the military. Air, Ground, Maritime, and Special Operations forces use JADOCS. It provides horizontal (across Services) as well as vertical (within Services) coordination of missions to ensure a common picture of targeting operational status across the entire joint force.

- Enables the Combatant Commands with the capability to plan and direct theatre counter-fire and precision strike operations through the real time synchronization with US and Coalition assets.
- Maximizes the Warfighter capability for rapid "system of systems" integration, visualization, coordination and deconfliction of critical mission information, which reduces the decision chain.
- JADOCS coordination and deconfliction spans Strategic, Operational, and Tactical levels.
- Complements the integrated Joint Warfighting Force by providing target selection, reporting, visibility, and handover capabilities to air, ground and sea elements across components and echelons, and vertically through hierarchies as desired.

Service Features:

As a software application, JADOCS can be configured and customized for each user and location.

In addition, these services include the delivery and maintenance of support thick client application:

- Manual Windows 10/11 installation
- Automatic Windows 10/11 deployment via SCCM
- JADOCS client VDI image

Service Ordering and Request: *[describes the procedure, which is required for customers to request the service or product; describes the means by which customers can report incidents and problems related to the use of the service or product – usually equal for all services, unless an exceptional procedure is required → this attribute will not be shown in the Catalogue, unless being exception from the standard for all services]*

Service Flavours: JADOCS Application Service can be delivered in various scale deployments, customised towards the size/echelon of the requesting HQ (Small/Medium/Large).

- JADOCS Software: includes all JADOCS software components, license, and documentation to have a full JADOCS site (server and clients).
- JADOCS Capability (Software+Support): includes the JADOCS software, license, documentation, and L2/L3 support to have a full set of functionality provided by the JADOCS server and client.

Available on: NATO Secret, Mission Secret, national secret

If you require availability of any other security domain please raise this as a New Service Request.

Service Prerequisites:

- NDW002 NATO Digital Workplace Service (High Side)
- INF004 - Infrastructure Virtualization Service

Standard Service Support Levels:

Service Availability¹ Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting: Standardised service reporting to customers in accordance with the NCI Agency SLAs

Available NCI Academy Training not covered by service cost:

Under Development	JADOCS Administrator Course - Focuses on the installation of the JADOCS software, configuration of the JADOCS Server and establishing the communication infrastructure between JADOCS nodes and external interfaces

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

Under Development	JADOCS Operator's Course - Focuses on the routine operations of the JADOCS workstation, the role of the Managers, and the functionality of the various menus

Service Cost / Price: The unit of measure for the Service is an HQ (small or large). The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP117 IOToolset Service

Service ID: APP117

Service Name: IOToolset Services

Portfolio Group: Application Services

Service Description: This service provides an online test management solution application to assist with IT technical Interoperability testing. The Service include the installation, support and update of variance available instances of the IO Toolset application. It also includes the repository of data needed to execute interoperability test events as well as options for training and enhanced support.

Value Proposition:

The IOToolset Service offers the tools, repository data, tool training, tool support, and tool maintenance. It supports the complex planning, execution and analysis and reporting of interoperability test events in a consistent way with a strict separation of concerns between the roles of users in a test event.

The IOToolset enables the following:

- Management of the test case repository
- Capturing of the CIS Planning for a test event
- Creation of interoperability test plans and test executions
- Capturing of test data in support of test executions
- Capturing of test results from the participants in a test event
- Reporting and analysis of the test results

Service Features:

The service features includes all the following components but the activities for each feature may vary depending on the service flavour:

- **Hosting:**
 - Installation
 - Configuration
 - Updates
- **Toolset Support:**
 - 1st level support related to issues with and the use of the toolset.
 - 2nd level support related to issues with and the use of the toolset.
 - 3rd level support related to issues with and the use of the toolset.
- **Training:**
 - Various Trainings for the different user community using the toolset.
- **Repository:**

- Includes the basic repository data consisting of test artefact including:
 - Interoperability test cases and requirements in support of Spiral 3, Spiral 4 and NATO testing as developed by the corresponding CIAV.

Service Flavours:

To obtain the IOToolset, it is required to first chose the desired instance(s) and include setup if mandatory and any desired options. The following flavours are available

- **APP117-1 Customer Managed instance:** Only available on nationally managed networks
 - Software Maintenance
 - Repository Maintenance
 - 3rd level toolset support
 - NOTE: If it is the first time requesting this flavour, it is recommended to include the system administration training
- **APP117-2 NCIA Managed NU instance:** Only available on NATO Managed Networks
 - Instance hosting
 - Database hosting
 - Internet facing security services
 - SSL certificates
 - Cyber hygiene
 - Instance monitoring
 - Backup & Restore
 - Software Maintenance
 - Application upgrades based on available releases
 - Repository Maintenance
 - Loading and updates of the repository data
 - 1st, 2nd and 3rd level toolset support
- **APP117-3 NCIA Managed Classified instance:** Only available on NATO Managed Networks
 - Instance hosting
 - Database hosting
 - Cyber hygiene
 - Instance monitoring
 - Backup & Restore
 - Software Maintenance
 - Application upgrades based on available releases
 - Repository Maintenance
 - Loading and updates of the repository data
 - 1st, 2nd and 3rd level toolset support
- **APP117-4 Setup*:**
 - * *Mandatory for Customer Managed and NCIA Managed NU instances*

- Server Installation and Configuration
 - Software Installation and Configuration
 - Setup Networking and Security (DNS, SSL)
 - Repository Package Delivery
 - Configuration Management
 - Setup backup & restore
 - Consulting and initial support
- **APP117-5 Training (optional):** Training is available on-site or remotely over Microsoft Teams.
 - System Administrator Training
 - Test Director Training
 - Test Coordinator Training
 - Tester Training
 - Configuration Management Training
- **APP117-6 Premium Support (optional):**
 - Increased monitoring of our support channels
 - Increased responsiveness to support requests from 2 days to 4 hours
 - Direct access to Toolset specialists

Service Request:

- Through a CRF if the customer is external or by providing billable funds from an existing NCIA project.

Available on: NATO Managed Networks and Nationally Managed Networks

Service Prerequisites: N/A

Standard Service Support Levels:

IO Core Toolset Support	Regular Average Response Time*	Premium* Average Response Time*
Level 1 support	2 days	4 hours
Level 2 support	2 days	4 hours
Level 3 support	2 days	4 hours

** based and available on core office hours in Netherlands.*

Service Cost / Price:

- The cost of each IOToolset instance are monthly based plus any required installation and options.
- Set up Costs are Mandatory for first time customer or if previous instances was uninstalled for Customer and NCIA Managed NU instances.
- Requests can be made of 6 months or 12 months durations only unless paired with TST002 Interoperability Testing Service with an event flavour.

- A request for a second instance at the same time will result in a discounted rate for the lowest costed instance.



Security Services

This page is left blank intentionally

SEC001 Security Accreditation Support Service

Service ID: SEC001

Service Name: Security Accreditation Support Service

Portfolio Group: Security Services

Service Description: The Security Accreditation Support Service provides guidance and support for security accreditation and re-accreditation activities for active and pipeline Communications and Information Systems (CIS), including support for the preparation of documentation required to facilitate Security Accreditation.

Value Proposition: Support to Cyber Security - Assessment. This service enables the reduction of security risk to the NCI Agency CIS and NATO Enterprise CIS, ensuring Cyber Security Policies, Architectures and Acquisition strategies, internally and externally, are coherent and effective. Additionally it provides assurance and stability of a well understood regulatory framework by all stakeholders.

c

Service Flavours: The Service is available in the following flavours:

- **Security Accreditation Preparation and Documentation (New Systems):** As described in the Service Feature. This flavour must be funded by each project that is seeking to achieve accreditation.
- **Security Accreditation Support (In-service systems):** As described in the Service Feature.

Service Available on:

Network neutral

Service Prerequisites:

- For new CIS and extension of CIS in service:
 - Validation of operational requirement.
 - Acceptance via NCSC Business Intake

Underlying Services: OTH001, SEC020, SEC101, SEC102, SEC104, TRA002

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery for In-service Systems.

SEC004 Cyber Security Analysis Service

Service ID: SEC004

Service Name: Cyber Security Analysis Service

Portfolio Group: Security Services

Service Description: Cyber Security Analysis Service is responsible for collecting and analysing digital evidence and threats (malware code) using a variety of specialized tools and techniques and a wide-variety of data sources and physical and virtual assets. The service is a cornerstone to support efficient Incident response, as well as to help fine-tuning detection and leverage expansion actions and threat hunting campaigns. The service provides technical analysis outcome and artefact for further Cyber threat assessment and for sharing with the NATO bodies, NATO nations and the other NATO partners within the agreed frameworks. The service also support the mitigation, remediation and post-incident phases.

Value Proposition: Support to Cyber Security - Defence. This service provides greater insight into potential security threats that contribute to lowering business risks. Furthermore informing better future prevention strategies obtained through a deep understanding of the nature of malware and forensic analysis.

Service Features: Cyber Security Analysis Service is comprised of the four following elements:

- **Forensic Analysis:** Performs online (OCF) and stand-alone (SCF) computer forensics analysis for Incident Management and on-request for specific use case.
- **Malware Analysis:** Carry out technical analysis on suspicious application code to identify any malicious content. Sharing of technical characteristics of malware within a trusted community either on an *adhoc* basis or via an automated MISP platform.
- **Evidence Acquisition:** Acquires in a forensically sound manner a variety of data source, physical or virtual assets for further processing by authorised NATO bodies.
- **Compromise Assessment¹:** Provision of resources during or post incident analysis to validate that a customer's systems and/or information (i.e. document set, database content) are free of malware.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO Mission networks (not C-SLA funded)

¹ Compromise Assessment is currently limited to those customers who may require this service feature as part of incident response. Specific requests from customers to confirm "clean" data received from third-parties is considered a new requirement and is not supported. Surge capacity for this service feature, via support from industry, is currently not funded.

Service Prerequisites:

Analysis activities require the provision of resources to ensure that all NCSC Operational Applications are maintained to ensure they meet optimal performance, can include but not limited to, sensor tuning, signature updates, application updates, performance tuning, forensics agents deployment and connectivity to NS, NR, NU, MS.

SEC029 delivers the PaaS to host SEC004.

Underlying Services: OTH001, TRA002, PLT008-3, PLT008-17, PLT008-21, SEC020, SEC101, SEC102, SEC104

Mandatory Dependencies:

SEC006 Cyber Security Incident Management Service

SEC007: Cyber Security Monitoring – perform network and log analysis

SEC008: Cyber Security OPCEN – coordination and 24/7 availability

SEC010: Cyber Security Information Sharing – sharing of cyber threat intelligence to NATO and NATO nations

Standard Service Support Levels:

Support Hours: Cyber Security Analysis service is available 24/7, 365 days per year, aligned w/ NCIA business hours for on-site support (Mon-Thu 08.30-17.30, Fri 08.30-15.30), The service is available outside of business hours including weekends/holidays via Cyber Security OPCEN (NCN 626 6666, see service SEC008). During these outside hours, the on-call support includes the recall of on-call staff in the office on decision of the On-call SEC006 Cyber Incident Responder.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC005 NATO Cyber Defence Rapid Reaction Team

Service ID: SEC005

Service Name: NATO Cyber Defence Rapid Reaction Team

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: Provides rapid, technical cyber defence assistance to NATO organisations and to individual NATO Allies subject to Council decision on a case-by-case basis. The RRT's foundation is the provision of multiple teams of NATO cyber experts but it can reach into NCI Agency's staff for deep expertise in order to deploy capabilities similar to those of the NCSC, but at remote locations and in response to Cyber Security incidents and crises.

Value Proposition: Support to Cyber Security – Defence. The Cyber Defence RRT provides flexible, deployable Cyber Security response where in times of crisis.

Service Features: The NATO Cyber Defence RRT is comprised of the following elements:

- Digital Forensics
- Malware Analysis
- Event/security Log collection
- Intrusion Detection System
- Full Packet Capture
- Online Vulnerability Assessment
- Incident Management
- Threat hunt
- Compromise assessment
- Advise and assist support
-

Service Flavours:

Deployed
Distributed
Centralized NCSC response

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

NATO nations networks (on a Council-approved, case-by-case basis)

Service Prerequisites: N/A

Underlying Services: OTH001, SEC020, SEC101, TRA002



Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC006 Cyber Security Incident Management Service

Service ID: SEC006

Service Name: Cyber Security Incident Management Service

Portfolio Group: Security Services

Service Description: Cyber Security Incident Management Service delivers cyber incident response according to the NATO Office of the CIO (OCIO) Cyber Incident Response Plan (CIRP). The service aims at delivering an efficient and effective response for containing, analysing and removing the threat, coordinating the restoration of the affected services within NCSC, NCIA and the stakeholders in the various NATO bodies, NATO nations and the other NATO partners within the agreed frameworks.

Value Proposition: Support to Cyber Security – Defence. This service provides a centralised Incident Handling and Response. The experienced, effective and efficient management of identified incidents through Cyber Security Incident Management Service ensure correct handling through incident lifecycle, in turn strengthening cyber security capability and therefore the overall effectiveness and productivity of the organisation.

The service is supported by the Cyber Operations Management System (COMS), implementing the Incident Management processes in accordance with the CIRP as well as providing a supporting platform for Information and Knowledge Management (IKM), hosting all the Standard Operating Procedures and Instructions. COMS is available for all NATO stakeholders on NATO Secret, and to NCSC on the NATO Restricted. COMS is funded as part of SEC006.

Service Features: The service is composed of: Incident Triage; Containment Eradication;; Alerting, Reporting, and Assisting with Recovery and Follow-up; The service also includes the management of and contribution to Cyber Incident Task Force (CITF).

Service Flavours: The Service is available as a single flavour.

Service Available on:

- NATO Unclassified
- NATO Restricted
- NATO Secret
- NATO Mission networks (Not C-SLA funded)

Service Prerequisites: On-Line and On-site support, including logistical, security, technical and political coordination.

Underlying Services: INF046, OTH001, SME005, TRA002, SEC020, SEC101, SEC102, SEC104

Mandatory Services

SEC004: Cyber Security Analysis – perform forensic and malware analysis



SEC007: Cyber Security Monitoring – perform network and log analysis

SEC008: Cyber Security OPCEN – coordination and 24/7 availability

SEC010: Cyber Security Information Sharing – sharing of cyber threat intelligence to NATO and NATO nations.

SEC029: Cyber Security Platform and Infrastructure Service. Provide the infrastructure on which all mandatory supporting cyber security services (SEC004, SEC007, SEC008, SEC010) are running.

Standard Service support levels: N/A

Service Availability: 24/7

Maintenance Services: no set schedule

Support Hours: Cyber Security Incident Management service is available 24/7, 365 days per year, aligned w/ NCIA business hours for on-site support (Mon-Thu 08.30-17.30, Fri 08.30-15.30), The service is available outside of business hours including weekends/holidays via Cyber Security OPCEN (NCN 626 6666, see service SEC008). During these outside hours, the on-call support includes the recall of on-call staff in the office.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC007 Cyber Security Monitoring Service

Service ID: SEC007

Service Name: Cyber Security Monitoring Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The Cyber Security Monitoring Service provides the monitoring of networks, websites and email traffic to detect and identify threats and compromises, and so to ensure cyber security.

Value Proposition: Support to Cyber Security – Defence. This service is designed to detect incidents – as a prerequisite to incident response. By monitoring hundreds of millions of events each day feeding a Security Incident and Event Management (SIEM) and processed by NCSC-maintained correlation rules, the Cyber Security Monitoring Service delivers cyber security of NATO CIS by providing assurance that:

- Email data spillages are detected and minimised
- Monitored website in question is available and undefaced
- Events will be correlated and scrutinised by qualified and experienced Security Analysts for appropriate actions as required

Service Features: This service is comprised of the following elements:

- **Internet Facing E-Mail Content Monitoring:** The provision of the ability to check all Inbound/Outbound Internet e-mail to ensure compliance with NATO and applicable local Security Policies; such checks include malicious code, executable content, encrypted content, SPAM, and Classified Data content. Outbound e-mail can be monitored either centrally by NCSC, or locally by appropriate IA Staff.
- **Internet Web Site Monitoring:** The ability to centrally monitor customer's Internet-facing Web Sites for unauthorised changes and to take appropriate reporting/remedial actions.
- **Network Monitoring:** Network Intrusion Monitoring, Detection & Prevention is the provision of centrally managed and monitored Network-based and Host-based technologies and feeds, for instance Network Intrusion Detection/Prevention systems, Application-aware firewalls, Web proxies and reverse-proxies, antimalware products, security and system logs, actionable threat intelligence, etc.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM Networks

Service Prerequisites:

SEC011 – Gateway Security Service

Provision of resources to ensure that all NCSC Operational Applications are installed and maintained to ensure they meet optimal performance, can include but not limited to, sensor tuning, signature updates, application updates, and performance tuning.

Provision outage and change notifications in order to minimise false-positives.

This service must be activated in conjunction with SEC006 (Incident Response), SEC004 (Technical Analysis) and SEC010 (Information Sharing). They are mandatory dependencies.

This service relies on the PaaS and SaaS delivered by SEC029, a mandatory dependency.

Underlying Services: OTH001, SME005, TRA002, PLT008-3, PLT008-17, PLT008-21, SEC020, SEC101, SEC102, SEC104

Standard Service Support Levels:

Service Availability Target: N/A

Service Restoration: 2 business days.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC009 Cyber Security Strategic Outlook and Outreach Service

Service ID: SEC009

Service Name: Cyber Security Strategic Outlook and Outreach Service

Portfolio Group: Security Services

Service Description: Cyber Security Strategic Outlook and Outreach Service:

- helps the NCSC leadership predict the evolution of the overall environment in which the NCSC operates, capture substantiated assumptions that inform and cohere planning activities, identify guiding principles to be used in day-to-day decision-making at all levels, and initiate long-term efforts that help ensure continued excellence in a fast changing environment
- Supports outreach in order to support CS SL development and, where appropriate, broader NATO Cyber Security aims. Encourages liaison and information sharing through outreach programmes and distribution of regular Cyber Security reporting, including Vulnerability Assessments and Cyber Sitreps. Outreach, including contribution to Cyber Sitreps, briefings, portals and other information campaign activities.
- Risk Communication and Education: Educate all relevant stakeholders to understand the risk associated with using the CIS for the objectives currently being undertaken.

Value Proposition: Support to Cyber Security – Inform. This service enables improved cooperation between Cyber security entities, better representation of cyber security domain and improved representation of Cyber security requirements and priorities. Risk Communication and Education educates relevant stakeholders to understand the risk associated with using the CIS for the objectives currently being undertaken.

Service Features: This service is comprised of the following features:

- **Cyber Security Strategic Outlook:** Establish and maintain the NCSC long-term planning assumptions. Elaborate the NCSC evolution policy and propose correcting actions by integrating the general context of Cyberdefense in connection with Transform branch, CTO, ACT, DIANA and OCIO
- **Cyber Security Outreach:** Supporting outreach in order to support CS SL development and, where appropriate, broader NATO Cyber Security aims. Encouraging liaison and information sharing through outreach programmes and distribution of regular Cyber Security reporting. Outreach, including contribution to stakeholder engagement, briefings, contribution to NATO Cyber Training, portals and other information campaign activities.

- **Risk Communication and Education:** Educate all relevant stakeholders to understand the risk associated with using the CIS for the objectives currently being undertaken.

Service Flavours: This Service is available as a single offering.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Underlying Services: OTH001, TRA002, SME005, SEC020, SEC101, SEC104

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC010 Cyber Security Information Sharing Service (CSISS)

Service ID: SEC010

Service Name: Cyber Security Information Sharing Service

Service Type: Customer Facing

Portfolio Group: *Security Service*

Service Status: Available

Service Description: The timely, secured and automated collection and dissemination of technical and/or contextual cyber security information using a variety of technologies.

Value Proposition: Support to Cyber Security – Inform. The sharing of timely and accurate information from and to a wide range of Cyber stakeholders (NATO bodies, NATO Allies and Partner Nations, Industry and Partners organizations) is essential to maintain the cyber security strength of the organisation, as a proven way forward to increase/maintain security posture, respond to Cyber Incidents and support Defensive Cyber Operations (DCO).

Service Features:

- Provide a central point for technical and automated information sharing, notification and communication to and from the cyber stakeholders community.
- Leverage web-based automation and Application Programming Interfaces (API) to deliver a range of technical services and consumer-facing services, focused on technical and actionable data.
- Complies with NATO STANAG 5660 to ensure Federated Mission Network interoperability
- Move towards a data-centric approach to maximise the ability to do secure information exchange and automated information exploitation.

Service Ordering and Request:

- This service can only be purchased under the ACO Centralized Service Level Agreement (CSLA) on behalf of the communities identified by each service flavour.

Service Flavours:

- **Cyber Defence Information Sharing (CDIS):** An extended service from the Malware Information Sharing Platform (MISP), covering Cyber Defence-relevant information (e.g. indicators of compromise, threat actors infrastructure and tactics, technics and procedures (TTPs), vulnerabilities etc) and enabling sharing among NATO, Nations and industries – compliant with NATO STANAG 5660 – Cyber Security Information Sharing.

This flavour is provided as:

- a set of 2 instances of **Multinational MISP (MN MISP)** supporting the MN MISP Smart Defence project, led under the governance of the MN MISP Smart Defence Steering Board on NATO Unclassified;

- a **Partners MISP** to industries (having signed the Industry Partnership Agreement - IPA) or similar NATO agreement for technical information sharing and other partners (i.e. CERT-EU) on NATO Unclassified;
 - an **unclassified MISP (NCSC MISP)** to NATO Cyber Security Community of Interest on NATO Unclassified;
 - a **classified MISP (C MISP)** to the NATO and Allied Nations Cyber Security community of interest on NATO Secret.
- **Cyber Security Threat Feeds (CSTF)** : Through the use of a centrally delivered lifecycle management, the CSTF is a fully managed service offered to all NATO bodies aiming at providing the best value for money in handling the procurement, the access management, the sharing of best practices among cyber stakeholders and the monitoring of license use for a wide range of industry-provided "Cyber Threat Intelligence and Cyber Security online tools".

Available on:

- NATO Unclassified (CDIS, CSTF)
- NATO Secret (CDIS)

Service Prerequisites:

- SEC029 Cyber Security Platform and Infrastructure Service delivers the PaaS to host some CDIS instances
- SEC035 Cyber Security FAS delivers Information (wiki) and Process Management to support both service flavours.

Underlying Services: OTH001, TRA002, SEC020, SEC101, SEC102

Standard Service Support Levels:

CDIS Service Availability¹ Target: 99% availability for all MISP instances.

CTSF Service Level:

- All users are granted resource access after having signed the Terms of Use in agreement with all cyber stakeholders
- The user management process has as maximum time for completion of 4h (during business hours) - provided the necessary information is available.
- Each purchased product are evaluated by the cyber stakeholders for their "value for money" with a set of bespoke metrics.
- Each of the purchased product license will be adapted to the current and planned usage, on one hand by sharing the use cases amongst stakeholders for a potential better use of the product, on the other hand by monitoring the use of the license to assess if the licence must be renewed, increased or decreased for next year's budget.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

**Minutes available during agreed reporting period excluding planned maintenance minutes*

**Service Restoration:**

Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting:

Standardised service reporting to customers in accordance with the NCI Agency SLAs

Available NCI Academy Training not covered by service cost:

A0757 NATO Cyber Information Sharing and Situational Awareness course

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC011 Gateway Security Service

Service ID: SEC011

Service Name: Gateway Security Service

Portfolio Group: Security Services

Service Description: Gateway Security Services provide a secure interconnection of different networks or network sections in order to protect an organization's key information.

Service is comprised principally of the following technical components: Data Diodes, Firewalls, Guard, Mailguard and VPN.

Value Proposition: Support to Cyber Security - Prevent. Expert and effective Gateway Security management is a fundamental cyber security requirement, preventing compromise and facilitating secure connectivity.

Service Features: This service is comprised of the following elements:

Common to all:

- Configuration Backup
- Disaster Recovery / Business Continuity Services / Service Restoration
- Log forwarding to archiving and/or forensic systems
- maintenance of system software (not XLG)
- 24x7 device health and availability monitoring
- Device troubleshooting
- Documentation
- CCP / AFPL process for software updates
- Provide 365 days on-call support for high incidents
- Annual test and review of BCP
- Development of SOP for repetitive activities (level 1, limited level 2)
- Education/training/familiarization of other teams
- Audit, accounting, authorization
- Incident management, troubleshooting

Gateway Security – Firewall Services:

- Support of physical, virtual and cloud-based firewalls
- Access to firewall configuration and near real-time logs
- Policy management (unlimited policy changes, following ITSM requests)
- Device management (bi-annual FW software update, weekly security content updates, emergency updates)
- VPN support (Site-to-Site, Client/SSL VPN)
- (limited) Network Access Control configuration for the Client VPN
- Access configuration for Client VPN
- Exercise adaptation / policy and configuration management (CSLA covered exercises)
- Firewall rule review and recertification, removal of unused/no longer required rules
- Reporting of allowed services / Provisioning of current rule set to SAA

- Security Incident Management support
- Application of the incident response activities (blocking hosts, disconnecting networks, NIMBLs)
- Development of custom application signatures
- testing/evaluation of new features and capabilities
- Post deployment network adaptations and expansion (SRTS)

Gateway Security – Mailguard Services:

- Adaptation of release markings
- Adaptation of email attachment types
- Patch installation
- Mailguard software upgrades
- Troubleshooting connectivity issues
- (limited) End-user support to identify mail rejection issues
- Testing/evaluation of new features and capabilities

Gateway Security – VPN Services:

- routing / tunnel configuration for NAFI and BMD-NAFI

Gateway Security – Guard Services:

- configuration of additional FAS flows
- adaptation of release markings

Gateway Security – Data Diode Services:

- configuration of new flows (SMB)
- configuration of new email domains

Gateway Security – IEG-C Services:

- configuration of new flows and access requirements
- adaptation of release markings
- patch installation
- system software upgrades

Service Flavours: Gateway Security Services comprise of the following flavours:

- **Firewall** covers LAN-WAN or Segmentation gateways; it can include NIPS integration or the establishment of Client to Site or Site to site VPNs
- **Mailguard** covers the secure email exchange between NATO and Mission networks (as part of an Information Exchange Gateway (IEG-C))
- **Guard** covers the secure data exchange between NATO and Mission networks (as part of an Information Exchange Gateway (IEG-C))
- **Data Diode** covers the unidirectional flow of data from a network with a lower security classification to a network with a higher security classification

- **VPN** covers the support of Community of Interest (COI) separation on the NATO Secret network
- **IEG-C** covers additional secure data exchange mechanisms (Web Proxy and RDP Proxy) between NATO and Mission networks, delivered by the NSP008648 project.

Service Available on:

Public Cloud
NATO Unclassified/Restricted
NATO Secret
NATO AOM networks

Service Prerequisites: Gateway Security Services depend on the installation of appropriate network infrastructure.

Underlying Services: OTH001, SME005, SEC020, SEC101, SEC102, SEC104

Standard Service Support Levels:

Service Availability: 24/7

Service Restoration: 2 working days

Maintenance Services: Tuesdays and Thursdays between 19:00 to 21:00 local time. SEC011 might be unavailable at selected sites in order to perform system maintenance and/or upgrades of the underlying operating systems

Support hours: Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC012 CIS Endpoint Protection Support Service

Service ID: SEC012

Service Name: CIS Endpoint Protection Support Service

Portfolio Group: Security Services

Service Description: Provision of expert guidance for the implementation, configuration and management of NATO Enterprise-wide endpoint security software. This guidance is used to harden NATO CIS against attack and compromise.

The endpoint security guidance consists of the following mandatory/optional controls, as per C3B Technical and Implementation Directive on CIS Security (AC/322-D/0048-REV3):

- Endpoint antimalware
- Host-based Intrusion Prevention (IPS)
- Secure web-browsing
- Desktop Firewall
- Application whitelisting
- Central management control for endpoint management
- Removable media protection
- USB Device Control protection
- Data-in-use Leakage Prevention
- Data-at-rest encryption
- Email antimalware
- Rogue Systems Detection
- Secure media erasure

Value Proposition: Support to Cyber Security – Prevent. The provision of CIS Protection Support enables coherent implementation of enterprise-wide endpoint security software, aligned to the policies and requirements of NATO that hardens the NATO CIS against compromise and is a proven way forward to increase/maintain security.

Service Features: The use of deep, niche expertise to deliver guidance for the implementation, configuration and management of NATO Enterprise-wide endpoint security software.

It includes:

- Full life cycle management for the respective endpoint security controls, ensuring the Approved Fielded Product List (AFPL) is updated.
- Reviewing and adapting the recommended configuration and guidance for every new minor and major release.
- Monitoring the threat landscape for emerging threats and provide mitigation at endpoint protection level.
- Monitoring the developments in endpoint protection and taking steps towards improving the cyber security controls.
- Reviewing and adapting the guidance for every new minor and major release.
- Providing 3rd-level technical support

- Assisting with vulnerability remediation, as suggested by local CIS Security Officers or revealed from a vulnerability assessment.

Service Flavours: The Service is available as a single flavour.

Service Available on: Network neutral

Service Prerequisites: N/A

Underlying Services: OTH001, SME005, SEC020, SEC101, SEC102, SEC104

Standard Service Support Levels: N/A

Service Cost / Price: The service is unitised based on the number of endpoints (workstations, servers, physical or virtual). For the price details, see the Service Rates document

SEC013 Crypto Compliance Support Service

Service ID: SEC013

Service Name: Crypto Compliance Support Service

Portfolio Group: Security Services

Service Description: Crypto Compliance Support Service provides assessment for Crypto Logistic Support and Maintenance and COMSEC Account management. It does this by providing formal inspections of all organisations storing, operating or maintaining NATO funded cryptographic equipment and NATO COMSEC Accounts in order to ensure compliance with established Directives.

Value Proposition: Cyber Security – Assess. Compliant cryptographic and communication security underpins the cyber security required within NATO and within the Allies. This service provides assurance that cryptographic installations are compliant with appropriate directives procedures and practices of COMSEC account custodianship are compliant with appropriate directives.

Service Features: The Service is comprised of the following elements:

Crypto Logistic Support, COMSEC Account and Maintenance Inspections:
Provision of formal inspection of all organisations storing, operating or maintaining NATO funded cryptographic equipment in order to ensure that the procedures and practices of account custodianship, cryptographic logistic support, installation and maintenance is compliant with established Directives.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Secret
NATO AOM Networks

Service Prerequisites:

Appropriate crypto and network access authority.

Underlying Services: OTH001, TRA002, SEC020, SEC101, SEC104

Standard Service Support Levels: N/A

Support Hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 6666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.00 Fri 08.30-15.00 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC014 Crypto Management and Logistic Support Service

Service ID: SEC014

Service Name: Crypto Management and Logistic Support Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: This service delivers management and logistic support required to securely implement and operate NATO's crypto solutions. This includes the management of the CARDS, EKMS, NEKMS, DKMI and Data at Rest IA Services, the Operational Control of the Crypto Forward Support Points and Cryptographic Keying Material Distribution, expert Device Procurement Support, and crypto integration and validation support.

Value Proposition: Support to Cyber Security – Prevent. Reliable management of crypto forward support. Delivery of authoritative functional, cryptographic expertise. Enabling of policy compliance and security, and the confidentiality, integrity and availability of data at rest.

Service Features:

CARDS, EKMS, NEKMS and DKMI Services

- Provision of resources to deliver the NATO wide accountability, receipt, transfer, supersession and destruction of cryptographic keying material and equipment.
- Maintenance of the CARDS Servers and authorisation for CARDS access to COMSEC custodians.
- Provision of specialist advice on cryptographic equipment installation, configuration, keying, operation, trouble shooting and related technical or engineering issues.
- Provision of the main point of entry for DACAN Key Management Infrastructure (DKMI) into NATO. Interface for DKMI to NATO EKMS (NEKMS) for NATO wide distribution of crypto electronic keys.

Data at Rest IA Services

- Provision of NATO Offline Crypto Equipment (NOLCE) keying Authority. Distribution and keying of all NATO Offline systems (Eclypt, SIR, Flagstone, etc.).

SECTRA Secure Voice Mobile Key Support

- Key Generation (KGC)
- Crypto Key and SECTRA Device management
- Assist remote sites during the keychange
- Replacement and re-introduction devices into the network
- Manual rekey of existing devices

Crypto Management and Logistic Support

- Cryptographic Device Procurement Support

- Advice on the design scope and planning for the procurement of NATO-approved cryptographic solutions, and execute the procurement and potentially provide the related services: implementation, training and maintenance.
- Operational Control of the Crypto Forward Support Points.
 - Provides Operational Control and Management of the Crypto Forward Support Points NATO-wide. Provision of timely replacement equipment and testing of faulty equipment prior to evacuation into the maintenance chain.
- Cryptographic Keying Material Distribution
 - The timely distribution of operational keying material and equipment to the end-user.
 - Allocation of keys to service requests (SRTS).
 - Provision of Controlling Authority services for all operational (theatre) and most operational (non-theatre) physical and electronic keying material.
 - Centralised management of distributed Crypto IP equipment providing the encryption of classified data (up to CTS level).

Cryptographic Integration Services

- Installation Site Survey: Provision of Initial Site Surveys in order to deliver specialist implementation and physical security advice prior to installation of cryptographic equipment or implementation of systems with a cryptographic component.
- Cryptographic Equipment Installation: Installation of Cryptographic Devices within Alliance and also individual Nations for end to end encryption ensuring installation and operation complies with current regulations, standards and directives. Installation of all types of cryptographic equipment, to include Voice, IP, Link, Trunk and Wide-Band.
- Production of IP Data Configuration Sheets: Production of user configuration data sheets for IP encrypted links.
- CIS System Management Support: Support to NCI Agency System Managers (and others) in the location, installation and on-site trouble shooting of systems, which include, but are not limited to, NNCCRS, SIGINT COINS, NNPS, NSWAN.

Cryptographic Validation Services

- Installation Inspection: Provision of installation compliance inspections and/or advisory visits on cryptographic installations in order to ensure compliance with current regulations, standards and directives.

Cryptographic Situational Awareness Service – (cost not included in v9.0 Service Rate)

Provision of Enhanced orchestration and maintenance of situational awareness by providing a tool (CSAT) to enable the following operational objectives:

- Provide a clear overview of cryptographic products and mechanisms currently in use.
- Enable the authorized users to perform orchestration of cryptographic activities ensuring management of products /capabilities during their entire life cycle.

- Support the production of operational impact analysis on current / future crypto capabilities as well as the definition of suitable operational mitigation / contingencies,
- Integrate information available in existing Authoritative Data Sources (ADS) to aid in the evaluation of the effectiveness and efficiency of cryptographic products available for NATO usage, as well as of the issues and risks associated with those currently in use.
- Incorporate an inventory of cryptographic products / mechanisms, allow the automatic production of the cryptographic issue mitigation action plan (CIMAP), and include a risk register to provide the commander with the ability to track status and take action as necessary.
- Provide the cryptographic stakeholders with an electronic “one stop shop” for cryptographic information by tracking (or providing links to) the following types of information (both in general for NATO-owned equipment and for national equipment that the nations want to have considered for future NATO use):
 - Inventory of algorithms and their lifetime / expectancy;
 - Approved crypto equipment;
 - Inventory of in-use crypto equipment;
 - Robustness assessment;
 - National notifications of decertification, such as end-of-life; and Issues and risks.

Review of Academy Cryptographic Courses

- Annual review of three cryptographic courses (A0004, A0006, A0067) that are delivered at the NCI Academy to confirm the courses continue to be fit for use and fit for purpose.

Coverage of CyOC Crypto Controlling Authority (CA) Duties

- In the absence of CyOC Crypto SME, NCIA NCSC will take over the following CyOC Crypto Controlling Authority responsibilities:
 - Take action on AIFS/AIMS formal messages addressed to SHAPE CyOC;
 - Authorize decrease/increase of Crypto keymat;
 - Take appropriate actions on COMSEC incidents.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Secret
NATO AOM networks

Service Prerequisites: Appropriate crypto and network access authority. Maintenance, repair of Crypto Equipment. Replacement of faulty crypto equipment on operational circuits. NATO wide Crypto delivery, accounting and key distribution system. The Data at rest IA Service is dependent on available and trained staff to operate, distribute crypto material.

Underlying Services: OTH001, SME005, TRA002, SEC020, SEC101, SEC102, SEC104

Standard Service Support Levels:

Service Availability: N/A

Service Restoration: 2 working days

Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 6666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1, meaning that the cost/price of the service is calculated on the enterprise total cost basis.

The service description is updated to include Cryptographic Situational Awareness in CCSC v9.0, however cost not included in v9.0 Service Rate. Pending confirmation from requirement owner.

SEC015 Security Certificate Service

Service ID: SEC015

Service Name: Security Certificate Service

Portfolio Group: Security Services

Service Description: Provides Certificate Authority, Revocation and Lifecycle Management of digital certificates/entities, including the appropriate training of registration authority personnel.

Value Proposition: Support to Cyber Security – Prevent. Secure connection and to authentication through digital certificate creation and management.

Service Features:

Certificate Authority Services for NS / MS, NU / NR and NMS: A service used for the creation and issuance of digital certificates to end-user (both human and non-human). This service will be provided from a Registration Authority (RA). The RA will be only interface to the NATO PKI system to create and issue digital certificates. The service provided also includes the revocation process. RA's will be installed locally to provide services to the end user both human and non-human. Manpower to operate Registration Authorities situated outside of the NATO Command Structure is not included within this service line. Manpower to operate Registration Authorities for non-eligible entities or exceptional-eligible entities not co-located with a NCS sites shall be provided by those external agencies or multinational entities.

Revocation services to NS / MS, NU / NR and NMS: CRL and OCSP services to NS/MS, NU/NR and NMS is a service used for providing a valid Certificate Revocation List and OCSP responses to end users, both human and non-human. The CRL provides a list of revoked certificates, this list will be checked, every time an end user uses digital certificates to establish a secure connection, or to authenticate to a system the CRL is checked. As soon as a certificate is on the CRL the connection, authentication is denied. OCSP responses provide the validity of a single end entity including the full chain in response to a specific query. The OCSP and CRL services to the aforementioned networks are a vital and critical service.

Lifecycle Management of Digital Certificates / Entities: Lifecycle Management of Digital Certificates / Entities is a service which contains the creation, issuance, management, maintenance, re-issuance, key recovery, revocation and deletion of a bonafide end-user (both human and non-human). The lifecycle management of digital certificates / entities also includes the partial management, maintenance of the meta directory on which the user are created.

Training of Registration Authority Personnel: Training of Registration Authority personnel is a service used for on the job training of Registration Authority Operators (RA Operators). On the job training takes place after the local site received a RA and the RA is configured and operational.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM Network
NMS

Service Prerequisites:

The connectivity to the Certificate authority on the desired network. The system is also dependent on available and trained staff to operate the RA.

Underlying Services: OTH001, SME005, SEC020, SEC101, SEC102, SEC104

Standard Service Support Levels:

Service Availability: N/A

Service Restoration: 2 working days

Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC019 Cyber Operations & Exercises

Service ID: SEC019

Service Name: Cyber Operations & Exercises

Portfolio Group: Security Services

Service Description: This service includes the contribution to the planning, coordination for, and execution of mission-based, cyber technical activities, in support of either a NATO exercise or operation. The service is provided through two distinct service flavours: through the participation of a generalist Cyber Planner (coordinator) in and towards the aforementioned activities contributions by a cyber-subservice specialist SME/capability, principally supporting exercises and DCO activities.

Value Proposition: Support to Cyber Security - Sustainment. Centralised SME services offer good value by having expert planning and coordination and leveraging the synergies of collocated deep skillsets. These also offer the efficiency of having cyber specialists available and resourced only when the customer requires them to contribute to cyber security sustainment and capability development.

Service Features: Cyber Operations and Exercise Service is comprised of the following elements:

1. **Cyber Security Support to Exercises:** Through a single point of contact coordinate the delivery of Cyber Security protection services and provide exercise development support for exercises identified within the CSLA in addition to the following, cyber-specific exercises:

Locked Shields
Cyber Coalition

Activities may include:

- Development of realistic and up to date cross-exercise technical storylines that facilitate the simulation of operational consequence management, simulate impact mission assurance and generate operational-level decision-making;
- Coordinate the alignment of cyber elements between exercises;
- Coordinate Cyber Security related concept development and experimentation during exercises;
- Coordinate operational exercise-support services (including NCSC Training Audience);
- Role simulation and exercise control activities;
- Coordination of Real life Cyber Security protection services in support of exercises including Gateway Security, Crypto management, Security Certificates, Incident Management and RRT.

The scale of these services provided to an exercise activity is subject to appropriate resourcing to meet the requested support, conducted through an agreed program of work.

2. **Support to Defensive Cyber Operations (DCO):** Comprehensive cyber defence policy has identified Defensive Cyber Operations (DCO) as a joint responsibility of the NATO Office of the CIO (OCIO), CyOC, and NCIA Agency. This service flavour provides a counterpart to CyOC and OCIO in order to:

- Receive, in a general manner, assistance and support in understanding how effective DCOs can be;
- Receive, in case of a request for DCO, the possible technical options NCIA could leverage with pros and cons and the side impacts;
- Upon approval of NCIA GM or any other authorized authority, execute and monitor the execution of DCO on NCIA networks;
- Confirm with CyOC the expected effect is achieved and regular reporting on the effectiveness;
- Monitor the NCIA-managed network to ensure no unplanned adverse effect are happening;
- Coordinate termination of the DCO when requested proof reading and drafting of the final report.

Service Flavours: The Service is available as two service flavours: a generalist Cyber Planner as a planning resource and effects coordinator; or as needed, a subservice SME and their more specialized contributions towards an exercise or operation.

Available on: Network neutral

Service Prerequisites:

None

Underlying Services: OTH001, TRA002, SEC020, SEC101, SEC104

Standard Service Support Levels:

Service Availability: Not applicable.

Service Restoration: Not applicable.

Service Cost/Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC022 Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service

Service ID: SEC022

Service Name: Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service

Portfolio Group: Security Service

Service Description: The Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) is an AirC2 specific service and secures the interconnection of Sensor and Flight Plan data sources provided at lower level of classification with Air Command and Control Systems (AirC2 systems). The ALF-SFP has been initially developed to satisfy requirements to secure the Air Command and Control System (ACCS) system boundary for sensor and flight plan data exchange but can be utilized for any other Command and Control System used in the Air Domain. In principle, the Service is leveraging a secured Trusted Computing Base providing hardening as well as Application Layer Firewall functions for a variety of similar security appliances. The ALF-SFP service is relying on a secured operating platform, data syntax validation and a hardened Application Layer Firewall. The Service provides unidirectional data flow from lower to higher level of classification as required to operate ACCS.

The ALF-SFP falls under the AirC2 governance for programmatic and configuration control aspects. In regard to cyber security evaluation and approval to operate, the ALF-SFP Security Service is under oversight of the ACCS Security Accreditation Board which might call for SECAN evaluation when deemed necessary.

Value proposition: Cyber security support to ensure integrity of sensor and flight plan data exchanged with the Air C2 System as well protecting the security boundary of the Air C2 system in regard to the interfaces supported.

Service Features:

The ALF-SFP is built on a secured Solaris platform utilizing the NISP Service (PLT013) and comprises a message syntax validation through proxies and an Application Layer Firewall as an evaluated security enforcing capability including required secured access to manage required components and interfaces.

The ALF-SFP service can be deployed and used in two scenarios:

- Stand-Alone ALF-SFP: The ALF-SFP supports handling and forwarding Eurocontrol ASTERIX and NATO STANAG 5535/ ADatP-35 compliant messages, as supported by ASIM (INF028), and it supports ICAO compliant Flight Plan Messages, as required for ACCS (APP050).
- ALF-SFP Service combined with ASIM (INF028) to ensure integrity of sensor data and to protect system boundaries against cyber threats.

Service Flavours:

- **NCS wide ALF-SFP** single SW baseline maintenance and In-Service-Support (ISS). The NATO ALF-SFP baseline maintained with this service flavour is a prerequisite for all other service flavours.
- **Site specific ALF-SFP** integration customised to local site specific requirements outside the NCS.

The ALF-SFP Service can be combined with ASIM (INF028) for sensor integration as required for the connected AirC2 system consuming sensor and flight plan data.

Available on:

NATO Secret to operate security protection functions and to connect to the AirC2 system and

NATO Confidential for Military sensor data sources and

NATO Unclassified for civilian Sensor and flight plan data sources.

Service Prerequisites:

PLT013 - NISP Service providing the standardized secured operating system

INF028 - ASIM Service either at the high or low side when combined with this security service

Hardware, software and connection requirements:

- Sensor data available at IP network level
- IP interface as part of the ACCS or Air C2 system
- Server hardware compatible to run NISP and authorized to host the ALF-SFP
- Network infrastructure

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

- Belgium +32 65 44 3177
- Netherlands +31 70 374 3177
- Italy +39 081 721 3177

- Germany +49 282 4978 3177
- USA +1 757 747 3177
- For NATO HQ +32 02 707 5858

Service Requests:

To request the SEC022 service, please complete the Customer Request Form and contact NCI Agency through the submit function included in the form following the link below.

https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

Functional unit	Service Level Target (availability)	Performance Thresholds
ALF-SFP single instance	99.5%	30 ms delay for passing data between ACCS and external systems

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
SEC022	Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service	NCS wide ALF-SFP software baseline maintenance and In Service Support (ISS)	1
SEC022	Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service	Site specific ALF-SFP installation	1

SEC023 Penetration Testing Service

Service ID: SEC023

Service Name: Penetration Testing Service

Service Type: Customer Facing

Portfolio Group: Security Services

Service Status: Available

Service Description: The Penetration Testing service seeks to test and improve resilience, assess compliance to security standards and identify vulnerabilities of NATO Communication Systems and Networks, through tailored security evaluation of CIS, websites, customer sites and communication equipment, in order to inform customers of existing vulnerabilities, allow remediation to occur and improve their security posture.

Value Proposition: Support to Cyber Security - Assessment. Principally, this service enables the customer to have a better understanding of their vulnerabilities and be able to remediate them before they can be exploited. Understanding vulnerabilities and resilience provides the necessary information to build an accurate picture of the security posture, and creates a baseline to measure progress of security improvements.

Service Features: Penetration Testing (NATO Type 4 Security Audit):

Tailored security tests against NATO networks and systems, with the objective to assess the impact of current cyber threats and techniques, as well as, their likelihood and difficulty of exploitation, on NATO CIS, a NATO Mission or NATO's cyber defences by emulating an intermediate or advanced cyber adversary. These unique activities are performed in support of accreditation, IT change management and software development assurance throughout the lifecycle of NATO CIS. A findings report is generated and provided to the customer at the conclusion of the test.

Service Flavours: The Service is available as a 3 flavours.

- **Web Application Penetration Test** – This test focuses on evaluating the security of a web application by simulating an attack from an unauthorized user or hacker. The aim of this test is to identify vulnerabilities, misconfigurations, and weaknesses in the web application, and to provide recommendations to improve its security posture.
- **Network/Infrastructure Penetration Test** – This test focuses on evaluating the security of a network/infrastructure by simulating an attack from an unauthorized user or hacker. The aim of this test is to identify vulnerabilities, misconfigurations, and weaknesses in the network and infrastructure, and to provide recommendations to improve its security posture.
- **Application Penetration Test** – This test focuses on evaluating the security of an application/software by simulating an attack from an unauthorized user or hacker. The aim of this test is to identify vulnerabilities, misconfigurations, and weaknesses in the application, and to provide recommendations to improve its security posture.

Available on:

NATO Unclassified



NATO Restricted

NATO Confidential

NATO Secret

NATO AOM networks

Service Prerequisites:

None

Underlying Services: OTH001, SEC020, SEC101

Service Reporting:

The customer shall receive a report 30 working days after last day of field execution.

Service Cost / Price:

The unit of measure for the service is per penetration test unit. A penetration test unit is defined as one week of testing conducted by a single resource. This standard applies uniformly across all penetration testing flavors, including Web Application, Network, and Application testing. The required level of effort may vary according to the complexity of the system or product being assessed, with a minimum requirement of one unit.

SEC024 Vulnerability Assessment Service

Service ID: SEC024

Service Name: Vulnerability Assessment Service

Service Type: Customer Facing

Portfolio Group: Security Services

Service Status: Available

Service Description: The Vulnerability Assessment Service seeks to test and improve resilience, assess compliance to NATO and industry security standards and identify vulnerabilities of NATO Communication Systems and Networks. It accomplishes this by the provision of resources to deliver on premise, holistic technical vulnerability assessments to support the identification, quantification of vulnerabilities in computer networks, systems (including Industrial Control Systems), hardware and applications.

Value Proposition: Support to Cyber Security Assessment for the NATO Enterprise and AOR. Vulnerability Assessments comply with NATO Security Policy and Directive that require periodic Cyber Security Audits and further define such assessment as mandatory minimum requirement for the risk informed decision during the accreditation process. It provides technical assessment data to the CIS Operating Authority for their risk management process. The assessment prioritizes vulnerabilities in their context of technical severity, exposure, using available contextual data such as the applicability of each vulnerability to threats, their potential impact on the organization and its mission.

Service Features: Onsite Vulnerability Assessment (NATO Type 3 Security Audit):

Execution of in-depth technical vulnerability assessments for NATO CIS networks against current threat landscape, NATO Policies & Directives, with root cause analysis, reporting and recommendations for remediation and mitigation.

It assess known software and configuration vulnerabilities which an adversary would exploit in a malicious attack against the CIS. The identified vulnerabilities are grouped into below MITRE ATT & CK Framework categories:

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement



Collection

Command and Control

Exfiltration

Impact

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

NATO Restricted

NATO Confidential

NATO Secret

Cosmic Top Secret A/B

NATO AOM networks

Service Prerequisites:

None

Underlying Services: OTH001, SEC020, SEC101, SEC104

Service Reporting:

The customer shall receive a report 30 working days after last day of field execution.

Service Cost / Price:

The service is unitised based on four variations (S, M, L, XL), with the determination of the variation based on the complexity of the scope to be assessed. The categories are defined by the scope of the assessment and applicable complexity.

Small (S) = 1 unit/credit | one network, <100 IP assets per network

Medium (M) = 2 unit/credit | one network, <500 IP assets per network

Large (L) = 3 unit/credit | one network, <1000 IP assets per network

Extra-Large (XL) = 5 unit/credit | one network, >1000 IP assets per network

SEC025 Emission Security Service

Service ID: SEC025

Service Name: Emission Security Service

Portfolio Group: Security Services

Service Description: The Emission Security Service seeks to assess compliance to standards and identify vulnerabilities, through the electronic evaluation of facilities processing classified information to establish their Facility Zone rating and subsequent vulnerability assessment of compromising emanations, in order to allow remediation to occur.

Value Proposition: Support to Cyber Security - Assessment. Principally this service enables the customer to have a better understanding of their vulnerabilities and so be able to remediate them before being exploited. Being able to understand any vulnerabilities and strengths also supports being able to build a picture of overall security, creating a baseline for measure progress to security improvements.

Service Features:

TEMPEST Facility Zoning: Provision of electronic evaluation of Facilities and Buildings where Classified information is processed in order to determine their Facility Zone Rating. Including advice to local IA staff on TEMPEST issues. The zone rating is provided with a technical report.

EMSEC Vulnerability Assessment: Provision of EMSEC vulnerability assessment within a Zoned Facility. The service includes advice to local IA staff on TEMPEST issues. The findings of the assessment is provided as a report.

Service Flavours: The Service is available as a single flavour.

Service Available On:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites:

None

Underlying Services: OTH001, SEC020, SEC101, SEC104

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC026 Attack Surface Reduction Service

Service ID: SEC026

Service Name: Attack Surface Reduction Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The Attack Surface Reduction Service provides Security Baselines, Vulnerability Monitoring and awareness, and Supply Chain Cyber Security. It delivers up-to-date Security Hardening Guides and support regarding their application to NATO CIS, analysis and evaluation of the recently discovered vulnerabilities affecting software and non-software CIS elements, and provides ad-hoc expertise related to CIS Component trustworthiness to system owners for their NATO CIS.

Value Proposition: Support to Cyber Security – Prevent. Security Hardening guides provides the NATO security baseline and minimal security posture required for a secure CIS, as per NATO directives and security best practices. Vulnerability management enables appropriate awareness of the CIS community related to the risk exposure NATO CIS is facing on a daily basis. Supply Chain Cyber Security constitutes an ad-hoc expertise capability, evaluating the level of trust that can be placed on a CIS component, based on the underlying deployed security measures in support of its development and maintenance.

Service Features:

Security Hardening Support: This service feature produces, delivers and maintains Security Guides for Software and Non-software products (Operating Systems, appliances) as part of the NCIA Change Management process. As such, Security Hardening guides constitute the minimal security baselines a CIS shall comply with. It also provides support to stakeholders on implementing the Security Guide on NATO CIS

Vulnerability Monitoring and Awareness: This service feature is composed of Monitoring of Vulnerability and Patch notification feeds and information channels; it assess relevance of known vulnerabilities to NATO CIS and to which extent they represent a risk for the organisation. The service includes publication of Weekly Security Bulletins which are relevant for NATO CIS, and Ad-hoc Security Bulletins which are relevant for NATO CIS (assessment of relevance to NATO, risk level exposure, identification of existing exploits, possible mitigations and remediation actions, recommendations regarding actions to be taken, identification of possible side effects and additional risks). The service also participates in NCIA patch management processes, including the "battleshort" procedure.

Supply Chain Cyber Security: Plan for, collect information about, assess, and handle the level of trust that can be placed in the components of a CIS based on the supply of sub-components, manufacturing, and logistics.

Service Flavours: The Service is available as a single flavour.



Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites: N/A

Underlying Services: OTH001, SEC020, SEC101, SEC102, SEC104

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC027 Continuous Security Posture Assessment Service

Service ID: SEC027

Service Name: Continuous Security Posture Assessment Service

Service Type: Customer Facing

Portfolio Group: Security Services

Service Status: Available

Service Description: The Continuous Security Posture Assessment Service delivers Continuous Security Posture Assessment, External Attack Surface Monitoring, and Active Directory Security Assessment to assess compliance to standards and identify software & configuration vulnerabilities on CIS components, communicate the results, provides advice and expertise on the appropriate resolution paths.

Value Proposition

The service provides Cyber Security Hygiene Indicators, by measuring the level of exposure to vulnerabilities of networked CIS components. It enables the remediation processes by identifying security shortfalls and delivering a mostly automated vulnerability picture from various potential points of attacks, together with a level of expertise regarding applicable protection measures to support reducing the potential attack surface.

Service Features:

External Attack Surface Monitoring: Provision of resources to continually assess the exposure of NATO CIS to the Internet. The findings and remediation recommendations are provided with the assessment report.

Continuous Security Posture Assessment: Provision of Continuous online Vulnerability Assessment to deliver audits of CIS infrastructures / systems to identify any vulnerabilities in software or configurations and to provide detailed reports containing cyber security hygiene indicators status, findings and prioritized remediation measures. Advising on mitigation techniques, escalating issues, with the objective of closing vulnerabilities at sites.

Includes the execution of the following checks:

Inventory of all connected devices

Inventory of authorized and unauthorized software

Inventory of patch and update status of all installed software and operating systems

Data Loss Prevention solution (DLP)

Secure configurations for hardware and software on workstations and servers

Malware defences and endpoint security mechanisms status

Secure configurations for locally managed network devices (limited functionality)

End of life Operating Systems and Applications

reports containing cyber security hygiene indicators status, findings and prioritized remediation measures. Advising on mitigation techniques, escalating issues, with the objective of closing vulnerabilities at sites.

Active Directory Security: Provision of assessment of an organisation Active Directory most critical vulnerabilities, Indicators of Exposure and Indicators of Attack, discover underlying issues and recommend courses of remediation.

Service Flavours:

The service is unitised based on four variations (S, M, L, XL) for the Continuous Security Posture Assessment service feature, with the determination of the variation based on the complexity of the scope to be assessed. The Service Delivery Manager reserves the right for final determination.

1. **SEC027-1:** Small (S) | one networks, <100 IP assets per network
2. **SEC027-2:** Medium (M) | one network, <500 IP assets per network
3. **SEC027-3:** Large (L) | one network, <1000 IP assets per network
4. **SEC027-4:** Extra-Large (XL) | one network, >1000 IP assets per network
5. **SEC027-5:** External Attack Surface Monitoring
6. **SEC027-6:** Active Directory Security Assessment

Available on:

NATO Unclassified

NATO Restricted

NATO Confidential

NATO Secret

NATO AOM networks

Service Prerequisites:

SEC029 delivers the PaaS to hosts SEC027 capabilities.

Underlying Services: OTH001 PLT008-3, PLT008-17, PLT008-21, SEC020, SEC101, SEC102, SEC104

Service Reporting:

The customer shall receive a report 10 working days after completion of the scheduled scan.

Service Cost:

The Continuous Security Posture Assessment service flavours are unitised based on four variations (S, M, L, XL), with the determination of the variation based on the complexity of the scope to be assessed.

The External Attack Service Monitoring service is unit 1.

The Active Directory Security Assessment service is unit 1.

SEC028 Remediation Support and Coordination Service

Service ID: SEC028

Service Name: Remediation Support and Coordination (RSC) Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The *Remediation Support and Coordination* Service provides the support and coordination of the cyber security shortfalls resolution process, following Vulnerability Assessments and pentesting activities executed on NCIA-managed CIS.

RSC provides visibility on the remediation and mitigation activities carried out under the overall NCIA Vulnerability Management process.

Remediation is a reactive measure taken after a vulnerability was discovered on a CIS (for instance from a Vulnerability Assessment report), and aiming at fixing security shortfalls by directly addressing their cause. This may involve patching a software vulnerability, removing a malware, or replacing a compromised device.

Mitigation is normally taken care of when no remediation option is available or actionable (zero day, software incompatibility with a patch, out of support devices...), as an urgent temporary security measure waiting for a proper remediation option, or as an additional feature to enhance the overall cyber security posture. This may involve restricting or removing access to some services, defining new Firewall or Intrusion Detection rules, reconfiguring a software, or implementing organisational and physical counter measures.

Value Proposition: *Remediation Support and Coordination* facilitates the resolution of security shortfalls, triggers and coordinates the NCIA response to security findings, and reports on the outcome of this remediation process.

It constitutes the coordination and vulnerability aggregation point that enables the resolution of identified security shortfalls across multiple business and technical areas.

By informing and reporting on the resolution process, it provides the customer a consolidated holistic visibility on the remediation actions.

RSC is executed:

- On a systematic basis after a Type 3 Security Audit;
- After a Type 4 Security Audit (*pentest*), when the scope is a system in operation.

RSC may also be executed upon specific requests after a major Cyber Incident or the execution of a Defensive Cyber Operation (DCOs), at the condition that the outcome of these events highlights the existence of vulnerabilities on the systems they address, and is limited in scope to NCIA-managed CIS.

Given the scale, the volume of relevant data, and the specifics of such reports, Continuous Vulnerability Assessment outcome (CVA, executed under SEC027 service) is outside the scope of SEC028.

While SEC028 coordinates the resolution process, the actual remediation and mitigation activities are not executed by SEC028, and are to be considered as part of the performance of other NCIA CIS delivery services.

Service Features:

Remediation Support: *Remediation Support* delivers technical expertise regarding vulnerabilities and to the remediation processes, and complements the outcome of Cyber Security Audits. It:

- Identifies possible remediation or mitigation options;
- Identifies and support Business Areas responsible for the remediation of the security shortfalls;
- Recommends priorities;
- Recommends resolution timelines;

Remediation Coordination:

- Executes the consolidation and coordination of the various activities to be carried out through a Remediation Plan;
- Represents the NCI Agency as focal point of the resolution process;
- Initiates the remediation process;
- Collects feedback from the Business Areas concerning the resolution options, timelines and actions.
- Coordinates with external stakeholders for the endorsement and the approval of the Remediation Plans

Remediation Report:

Remediation Report provides external visibility on the remediation actions. It:

- Informs and Advises external stakeholders (SAAs, CISOAs, OCIO...);
- Delivers reports and dashboards for ongoing remediation processes, and during a defined timeframe;
- Highlights the residual vulnerabilities not fixed within this timeframe;
- Provides ad-hoc expertise on vulnerability management;
- Ensures the data is presented consistently and under the same format, regardless of the types and specifics of Vulnerability sources.



Service Flavours: The Service is available as a single flavour.

Service Available on:

- NATO Unclassified
- NATO Restricted
- NATO Secret
- NATO AOM networks

Service Prerequisites: N/A

Underlying Services: OTH001, SEC020, SEC101, SEC102, SEC104

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1, and is mapped to the annual number of Security Audit reports requiring a Remediation Plan. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC029 Cyber Security Platform and Infrastructure Service

Service ID: SEC029

Service Name: Cyber Security Platform and Infrastructure Service

Service Type: Supporting Service

Portfolio Group: Security Services

Service Description: The Cyber Security Platform and Infrastructure Service provides the NCSC Core physical and virtualised CIS infrastructure - covering both Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). These services provide the underpinning building block layer for other NCSC dependent services (Cyber Security Monitoring & Incident Management / Online Vulnerability Assessment / NIPS & FPC / Online & Offline Computer Forensics / E-mail Filtering / Endpoint and E-mail Security). The infrastructure associated with the service is layered in 3 tiers: T1 in NNHQ Brussels / T2 in SHAPE MONS (NCSC core networks and appliances) and T3 (Remote NATO Sites) via dedicated NCSC enclaves.

Value Proposition: Support to Cyber Security – Sustainment. This service is a key enabler that enables NCSC to operate and provide its customer facing services.

Service Features: This service is comprised of the following elements:

- **Cyber Infrastructure-as-a-Service (IaaS):** NCSC's IaaS provides the physical and virtual infrastructure for hosting the set of tools required to deliver NCSC's portfolio of cyber security services.
- **Cyber Platform-as-a-Service (PaaS):** NCSC's PaaS provides the Operating System level hosting for the upper level applications and toolsets required to deliver NCSC's portfolio of cyber security services. This includes back-office functionality - i.e MS Office, E-mail and Business Continuity functions.

Service Flavours: The Service is available in two flavours:

1. **Central Services** – located in Mons, Belgium and constitutes the main Cyber Security Centre Operating capability.
2. **Tier 3 Enclaves** – located at remote Tier 3 sites to enable the effective monitoring, logging, scanning of remote networks.

Service Available on:

- NCSC Core Unclassified
- NCSC Core Restricted
- NCSC Core Secret
- NRoI Restricted

Service Prerequisites:

Provision of HVAC and Accommodation for NCSC central and deployed capabilities.

Underlying Services: OTH001, SME005, SEC020, SEC101, SEC102, SEC104

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table below.¹

	Availability Target	Service Restoration Period
During Support Hours	99.5%	4 hours
Outside Support Hours	99.5% (critical services)	4 hours

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

¹ Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. While this provides a standard availability target for the service, regional support arrangements and therefore the availability targets may vary and should be agreed during the SLA discussions.

SEC030 Cyber Threat Hunting Service

Service ID: SEC030

Service Name: Cyber Threat Hunting Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The Cyber-Threat Hunting service provides a threat-based detection and hunting capability through directed analysis of NATO CIS against a selected set of intelligence artefacts, Indicators of Compromise, predicted tactics, techniques and practices of Cyber Threat Actors (CTA), cyber criminals and insider threats. This set of actionable information is provided in a joint effort by SHAPE CyOC, JISD, OCIO and other relevant stakeholders according to the agreed NCSC-developed process. This allows identification of advanced attempts to compromise NATO CIS from threat actors knowledgeable enough to avoid automated detection techniques and provides a technical assessment that will inform the operational assessment and follow-on defensive activities. This service can be provided inside and outside the scope of Defensive Cyber Operations (DCO).

If reinforcement by industry partners is required, the supplemental cost will also be charged separately.

Value Proposition: Support to Cyber Security - Defence. The direct benefit of Threat Hunting is a reduction in average detection time through the proactive discovery of security incidents and/or adverse activity that evade usual detection methods, allowing early and coordinated response.

Service Features:

- **Asset Monitoring:** Configuration, collection and evaluation.
- **Technical Analysis:** Targeted Network Collection, Monitoring and Detection.
- **Correlation:** Tailored evaluation within a dedicated repository, search and analysis of malicious patterns and behaviours.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites: The execution of the service have technical prerequisites. Depending on the scope of the threat hunting, the necessary tools will need to be installed on the target network(s) and confirmed working before the Threat Hunting can occur.

Underlying Services: OTH001, PLT008-3, PLT008-17, PLT008-21, SEC020, SEC101

Standard Service Support Levels: N/A



Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC032 Adversary Emulation Service

Service ID: SEC032

Service Name: Adversary Emulation Service

Portfolio Group: Security Services

Service Description: The Adversary Emulation Service seeks to assess and improve the resilience of NATO Communication Systems and Networks, through tailored security evaluation of people, process and technology, in order to allow remediation to occur and improve their security posture.

Value Proposition: Support to Cyber Security - Assessment. Principally, this service enables the customer to assess and improve its resilience against an advanced attacker. Understanding vulnerabilities and resilience provides the necessary information to build an accurate picture of the security posture, and creates a baseline to measure progress of security improvements.

Service Features:

Adversary Emulation (NATO Type 5 Security Audit): Tailored red and purple teaming activities against NATO networks and systems, with the objective to evaluate and improve the resilience of NATO CIS, NATO Mission or NATO's cyber defences by emulating an intermediate or advanced cyber adversary. Adversary emulation mimics specific techniques, tactics and procedures (TTPs) used by known threat actors. Adversary emulators construct scenarios to test different aspects of an adversary's TTPs against a given target. These unique activities are performed in support of NATO missions and exercises. A security report is generated and provided to the customer at the conclusion of the test.

Service Flavours:

- **Red Teaming** – Objective based assessment to test the resilience of a target network, mimicking a malicious actor to assess the people, process and technology in terms of prevention, detection and response to a cyber-threat. In this flavour, the Red team tries to stay as stealthy as possible to assess the prevention, detection and response capabilities of a given target following the “train as we fight” approach.
 - **Small:** Small-scale red team engagement involves a small group of security professionals. The team uses a targeted approach to reach their defined objectives. This type of engagement is usually conducted in one phase of testing over a short period.
 - **Large:** Large-scale red team engagement involves a larger team of security professionals. This type of engagement is usually more comprehensive and can last for several months, during which the team conducts various tests and simulations to reach their objectives. A large red team engagement typically requires more resources, including personnel, time, and

specialized tools and technologies, and may involve multiple phases or stages of testing.

- **Purple Teaming** – Scenario based assessment to test the resilience of a target network, mimicking a malicious actor to assess the prevention and detection to a cyber-threat. In this flavour, the Red team works with the Blue team to assess the prevention and detection of each scenario.
 - **Security controls validation:** determines how effective deployed security technologies are, as an overall system of security systems. The main goal of security control validations is to assess and improve the detection and prevention mechanisms of a given system against TTPs used by threat actors targeting NATO.
 - **Baseline assessment:** benchmarks the detection and prevention mechanisms of a given baseline. The goal of a baseline assessment is to measure the effectiveness of new security technologies implemented on a defined baseline.
- **Phishing Simulation Campaigns** – Provision of resources to configure and execute phishing simulation campaigns directed at all levels of NATO staff. Phishing Simulation Campaigns aim at exposing staffs of all levels to the dangers encountered with modern communications methods and systems, by using the same targeting methods adversaries use with the intention of gathering information of specific target. The findings and remediation recommendations are provided with the campaign reports.

Service Available On:

NATO Unclassified
NATO Restricted
NATO Confidential
NATO Secret
NATO AOM networks

Service Prerequisites:

None

Underlying Services: OTH001, SEC020, SEC101

Service Reporting:

The customer shall receive a report 30 working days after last day of field execution.

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC035 Cyber Functional Area Service (CyFAS)

Service ID: SEC035

Service Name: Cyber Functional Area Service

Service Type: Customer Facing

Portfolio Group: *Security Service*

Service Description: CyFAS offers cyberspace-specific, operationally focused applications delivered as a fully-managed service to empower the Cyber stakeholders to obtain from NCSC data lake and other information sources the necessary Situational Awareness (SA), and to securely execute a variety of Cyber security processes across NATO organizational boundaries, notably in support to Cyber Incidents response and Defensive Cyber Operations (DCO).

Value Proposition: Support to Cyber Security – Inform. By leveraging the many sources of information collected by the NCSC sensors across NATO networks and the fusion of other collected information, CyFAS delivers a set of services in the form of dedicated and customizable dashboards relevant to the cyber stakeholders' area of interests, as well as a robust, secure and cross-organizational workflow-driven capability to implement NATO-wide cyber-related processes, primarily to support Cyber Incident Response and Defensive Cyber Operations (DCO).

Service Features:

- Provide a central point to execute cyber processes, using common source of information and references (e.g. site name, NATO structure, Point of contacts etc),
- Allow relations between processes (automatic trigger, information sharing) while respecting process ownership and need-to-know.
- Visibility and tracking of NATO Restricted process instantiations from NATO Secret systems for tighter integration with the Operational community.
- Move towards a data-centric approach to maximise the ability to do secure information exchange and automated information exploitation
- Leverage NCSC data-lake provided through SEC007 to deliver dedicated, customizable dashboard for Cyber Defence Situational Awareness.

Service Ordering and Request:

- Currently, this service can only be purchased under the ACO Centralized Service Level Agreement (CSLA).
- The availability of this Service for Deployable CIS is planned in the future – linked to the delivery of a Capability Package (CP).

Service Flavours:

- **Cyber FAS - Product Lifecycle** – This flavour includes Overall Service Management, licensing and system maintenance.
- **Cyber Defence Situational Awareness (CDSA)** – Aims at delivering the "Blue Picture" to the NATO Cyber stakeholders (ACO CyOC, OCIO...) through the delivery of overall Situational Awareness. It makes use of custom dashboards on Cyber

Incident filtering, known vulnerabilities, etc, with the ability from the customers to request adaptation to existing or creation of new dashboards and inclusion of new data sources to answer Cyber-focused questions and support decision-making.

- **Cyber Operations Management System (COMS)** - Collection of capabilities providing the creation, execution and auditing of complex workflows and processes where stakeholders are distributed across the NATO landscape and beyond. COMS is the supporting tool for Cyber Incident Response Plan (CIRP) and its associated processes. COMS also offers a supporting platform for Information and Knowledge Management (IKM), which can host all the Standard Operating Procedures and Instructions related to the associated processes, and authorizes concurrent editing of pages from personnel coming from different NATO domains.

Available on:

- NATO Restricted
- NATO Secret

Service Prerequisites:

- SEC007 is the mandatory source of information for CDSA
- SEC029 delivers the PaaS to host COMS and CDSA
- SEC034 ACPV will become a source of information to CDSA when operational.

Standard Service Support Levels:

Service Availability¹ Target: linked to the underlying availability of SEC029

Service Restoration:

Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting:

Standardised service reporting to customers in accordance with the NCI Agency SLAs

Available NCI Academy Training not covered by service cost:

A0757 NATO Cyber Information Sharing and Situational Awareness course

Service Cost / Price: The unit of measure for SEC035-1 Cyber FAS -Product Lifecycle flavour is 1. For all remaining flavours the cost model is composed of the number of users, the number of CDSA dashboards and the number of COMS Processes.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

SEC036 Cyber Portals Service (CyPS)

Service ID: SEC036

Service Name: Cyber Portals Service

Service Type: Customer Facing

Portfolio Group: Security Services

Service Description:

The Cyber Portals Service (CyPS) groups all NCSC-managed information portals supporting a wide-variety of NATO Cyber stakeholders. It serves as the central point for Information and Knowledge Management (IKM) for the cyber community and as a delivery mechanism for dissemination of information, communication and decisions.

Value Proposition:

By centralizing the different information sharing portals within the Inform Branch, the NCSC aims at consolidating the information and adopt a “capture-once, use-many” approach to the information. The extensive use of Federation services across multiple NATO networks, the automatic replication of information from different security domains, the common taxonomy and term stores are some of the key values the service is offering. Currently existing for the NCSC Information Sharing portals and the NIAPC, it aims at expanding its use of the wider Cyber community (NICC, NSAB, BCISOA, CRMG)

Service Features:

User Management: leveraging Active Directory Federation Service (ADFS) from different NATO networks for single-sign-on integration and better user experience.

Vendor Management: A secure section for vendors to submit and manage their products, including specifications and certifications.

Search and Filter Capabilities: Enables users to easily find products based on specific needs, such as functionality, certification, and classification.

Documentation and Support: Provides access to documentation, user guides, and customer support for vendors and project teams.

Service Flavours:

- **Cyber Portal – Product Lifecycle** - This flavour includes Overall Service Management, licensing and system maintenance. (qty 1)
- The **NATO Information Assurance Product Catalogue (NIAPC)** is an online service that allows external vendors to input, manage, and display their cyber defence products approved for use, in accordance with AC/322-D(2010)0042 InfoSec Technical And Implementation Directive For The NATO Information Assurance Product Catalogue (NIAPC). (qty 1)
- **NIAPC Processes Execution and Content Management:** the business processes execution of the requests from vendors to validate (with NATO Digital Staff, National CIS Security Agencies etc) and manage product lifecycle. Each unit covers 200 requests. (minimum qty 1)

- The **NCSC Information Sharing portals (Insight)** are used to publish and disseminate NCSC security products. It includes the Active Directory Federation Service (ADFS) to interconnect NCSC to other NATO networks. The portals are accessible from NU, NR AIS and from all NS environments. It will evolve to become the **NATO Integrated Cyberdefence Center (NICC) portals**. (qty 1)
- **The Portals information and content management** for all NCSC-managed communication and information platforms, including Cyber Incidents and Defensive Cyber Operations (DCO) support (qty 1)

The purpose of the NATO Information Assurance Product Catalogue (NIAPC) established under this Directive is to provide e NATO nations, and NATO civil and military bodies, a way to operate into a NATO compatible manner.

This platform will serve as a central repository of hardware options available for projects, facilitating decision-making regarding products selection, pricing, and procurement.

Available on:

- NATO Unclassified (Insight, NIAPC)
- NATO Restricted (Insight)
- NATO Secret (Insight, NSAB, BCISOA)

Service Prerequisites:

SEC029 delivers the PaaS to host NCSC Insight portals, the NASB and the BCISOA.

PLT010 (AWS) to host the NIAPC portal

Standard Service Support Levels:

Service Availability Target: 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 48 hours.

Service Reporting:

Standardised service reporting to customers in accordance with the NCI Agency SLAs

Service Cost / Price:

The cost model for all flavours is unitized cost model and the current demand in 2026 for each flavour is 1 .



Logistic Services

This page is left blank intentionally

LOG001 CIS Asset & Materiel Management Service

Service ID: LOG001

Service Name: CIS Asset & Materiel Management

Service Type: Customer Facing/Support

Portfolio Group: Logistic Services

Service Description: The CIS Asset & Materiel Management Service embraces all of the CIS Asset and Materiel Management activities that the CIS Sustainment Support Centre (CSSC) provides both directly to the Customer and internally as a support function to the Service Lines. CIS Asset and Materiel Management includes CIS equipment codification, database management, inventory management, receipt, dispatch, storage, stock management, warehousing, internal controls, handover takeover, equipment write-on/write-off, support to operations and disposal coordination. The CSSC performs as the single point of entry for the majority of new CIS equipment procured through common funding of NATO. In addition, CSSC provides Asset Management Subject Matter Expert Services directly to the Customer or internally to the NCI Agency Service Lines.

This service only includes the Agency's centralised resources required to deliver the service. Local support from collocated Agency staff in support of day-to-day operations is not included and must be funded locally. Albeit LOG001 pertains to services provided ONLY by CSSC, it will exceptionally be used as a transfer vehicle, so as to enable previous LEG008 funds and associated activities and responsibilities of the CSUs, to be transferred to DCSU.

Value Proposition: The Service provides multiple values:

- Provision of a central hub for most of CIS Asset and Materiel Management activities;
- NATO common funded CIS Equipment is managed and safeguarded throughout the full materiel lifecycle process;
- CIS equipment, and CIS Spares and Consumables for a number of years of Integrated Logistic Support (ILS) of CIS Systems and Capabilities are available to support NATO operations, exercises, and the static infrastructure, with significantly reduced time between requisition and delivery;
- Improvement of the CIS Materiel Management and availability of stock managed items;
- The centralization of the codification, storage, warehousing, receipt, dispatch, transportation, and materiel coordination functions provides cost savings to the NATO Nations. This includes both NSIP as well as the follow on Operations and Maintenance activities;
- In cases where Spares supporting in-service systems are likely to become 'diminished manufacturing availability', they are procured, stored and available for supply by the CSSC Warehouse in order to ensure NATO Business Continuity;
- For no longer required equipment CSSC, if deemed re-useable, can provide suggestion for central storage, return to service or local dispose;
- Reduced overall costs per item managed through the stock management process.

Service Features:

- **Codification:** Codification and management of item master data information that is used to support procurement, supply and material management of CIS Equipment purchased using NATO common funding. Codification is used within NATO in order to improve CIS/Non-CIS identification, supply and property accounting. Codification, if carried out correctly, will result in cost savings for NATO as assets will be more efficiently and effectively managed in support of NCI Agency Service provision. The codification is also executed NCI Agency non-CIS equipment and common elements of the AMDC2 System in support of property accounting tasks. Codification is divided into Codification of CIS Assets and Codification of Non-CIS Assets.
- **Planning:** Planning, scheduling, coordination and documentation update for Storage Management and Warehousing Services. Planning, scheduling and coordination for Receipt and Dispatch Services. Planning, scheduling and coordination for asset management SME services.
- **Receipt/Dispatch:** The CSSC performs as the mainpoint of entry for the majority of new CIS equipment procured through common funding of NATO. The Receipt and Dispatch (R/D) activities are an essential element, which supports project execution, service delivery, supply management, asset management and database management activities associated with CIS. CSSC also receives and dispatches non-Common funded materials on request from some Host Nations and MoU organizations. The receiving process, which is managed in the ORACLE Inventory/Order Management database is handled either directly or indirectly by the CSSC Receipt and Dispatch. This is an Asset Management activity providing identification, serialization and traceability of CIS equipment. CIS Materiel consignments are processed, prepared and dispatched through the R/D section of CSSC. Dispatch can include freight forwarding, special deliveries, urgent request and courier coordination services. R/D also coordinates the most suitable and cost effective transportation service in conjunction with NSPA. Although NSPA is responsible for the management of transportation of CIS Material on behalf of the NCI Agency, CSSC provides a single point coordination Service to our internal and external customers to ensure that material moves are managed efficiently and effectively. Transportation Requests are received and processed by CSSC to support the original customer requests (MR/IR/MOI etc.). R/D also manages classified equipment.
- **Storage:** Assets are stored and managed in the CSSC Warehouse as part of the Inventory Project supporting the procurement, supply, exchange, repair and upgrade processes for CIS equipment within the NCI Agency. The Service relates to the CIS requisitioning and supply activities of the NCI Agency.
- **Stock Management:** CSSC provides a Stock Management Service in conjunction with the Inventory Project of the NCI Agency. Planning, scheduling, coordination and documentation update for stock management service. Supply of CIS stock managed materiel in line with PM requisition requirements. Replenishment activities related to all stock Managed CIS equipment.
- **SME Services:** Provide customers with near real time management of CIS Equipment Account Balances associated with the Custodian Account and Depot Stock

Organization Structure. The inventory management service is an essential enabler of material management and property accountability. CSSC provides advice and support to the Operations and Exercise Service Line in the development of CIS Logistics related plans in relation to Exercise and Operational Planning. This planning effort may be dedicated to a specific Exercise/Operation or included within an existing SLA. CSSC provides expert logistics support to projects such as those related to the AMDC2 (AirC2/BMD) in the data capture and inventory setup/management of associated assets. CSSC conducts data cleansing activities in support of Projects/Programmes such as EBA and ITM. Although this is not meant to be a day-to-day activity, it is anticipated that this task will continue in excess of 12 months.

- **Inventory Management:** The indirect or direct support is provided to the Custodian Account holder in the completion of the annual inventory activities. The support activities are related to handling of discrepancies within an account balance list. This can be associated with the annual counting process or for an individual or multiple item loss/damage report.
- **Logistic Maintenance Support:** This is a required activity related to the accountability of CIS materiel that is returned by the customer for preventative or corrective maintenance actions or to storage for future reuse (reverse logistic). In these cases CSSC will conduct handover/takeover (HO/TO) checks of the property which includes full inventory of materiel prior and after completion of the maintenance activities.
- **End of Life asset management:** when an asset reaches his end of life (obsolescence, failure or loss), CSSC provides assistance in reporting, including pre-investigations, creation of Report Of Survey (ROS), in case physical handling of condemned equipment (palletizing, storage) and Write-off from the Book.
- **Support Planning** The HO/TO is an essential element of inventory checking when equipment is moved from the responsibility of one Sub-PAO to another or back to CSSC. The HO/TO process is required to ensure that common funded equipment is handled in accordance with the Financial Regulations and Asset Management Directives and Procedures.

Service Request: The Service may be requested in multiple ways:

- Identified within SLA / OLA;
- E-mail requests to Resource Management Branch Tasking Cell;
- EBA Project Management Milestone Request;
- EBA Internal Requisition;
- ITSM;
- EBA Work Request;
- EBA Move Order Transfer;
- EBA Internal Requisition;
- E-mail to Resource Management Branch Tasking Cell;
- Materiel Request through iProcurement.

Service Flavours: The Service is available in multiple flavours, depending on the required features and forms of support.

Available on: N/A

Service Prerequisites:

None

Underlying Services: OTH001

Standard Service Support Levels:

- **In House:** Equipment is stored, maintained and managed at the CSSC main warehouse and released and/or replenished on request from the relevant Service Line/Project Manager.
- **On Site:** Equipment is forward deployed to Buffer Stock locations in order to support the 'urgency' element of spares and consumable supply for Service Lines and PMs.
- **Routine:** Service provided as a routine process associated with standard timelines.
- **Urgent:** Service provided as a prioritized process associated with urgent requirements and timelines.
- **Codification:** All actions required for the execution and management of the codification will be conducted by the codification team within AMSB, CSSC.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

LOG002 Test Equipment & TEMPEST Level Testing

Service ID: LOG002

Service Name: Test Equipment & TEMPEST Level Testing

Service Type: Customer support

Portfolio Group: Engineering Services

Service Status: Available

Service Description: CIS Sustainment Support Centre (CSSC) Brunssum is NCI Agency single point of contact for all Test Equipment (TE) and Fibre Optic Reel (FOR) requirements, general maintenance, verification and repairs. This service entails initial acceptance testing of new procured TE and FOR, verification of calibration performed by external institutions, repairs and technical evaluation of items fulfilling manufacturer criteria to NATO standards. The service also entails equipment TEMPEST level testing to SDIP-27 standards under the technical direction of the NATO Cyber Security Centre (NCSC).

Value proposition: Conducting periodic maintenance and testing to ensure that all TE and FOR are safe to use, accurate to the original manufacturer's specifications, and traceable to back to international standards.

CSSC maintains the only TEMPEST facility within the NCI Agency conducting tests of commercial-off-the-shelf (COTS) CIS items used to process NATO CONFIDENTIAL and above.

Service Features:

- Testing and repair of TE and FOR to confirm manufacturer specification, performance and functionality.
- The periodic maintenance and testing of TE and FOR does not simply mean checking the specifications. A comprehensive function test and minor preventive maintenance are also performed, improving the reliability of the TE and preventing failures. At the same time, a firmware update will be performed to make sure the instrument has all the latest features.
- The standards used in the maintenance process are traceable to national and international standards or other intrinsic standards. The method and procedures used for certifying TE complies with most IEC/ISO 17025 and military requirements.
- All TE maintenance is performed either at the CSSC or at customer's location within a controlled environment room.
- Providing unbiased technical advice and engineering support, ensuring solutions are "fit for purpose" and "fit for use" whilst minimizing the cost to the customer.
- Performing mandatory Electrical Safety Inspection for compliance to NEN 3140 (standard for operation of electrical installations - Low voltage).
- Testing and evaluation of Electric Radiation (ER) signals for Compromising Emanation (CE) in order to allocate the appropriate SDIP-27 TEMPEST Level B or C rating.
- Acceptance testing of TEMPEST equipment certified by NATO Approved Suppliers to confirm that the equipment meets the SDIP-27 TEMPEST Level rating allocated.

Service Request: Assigning an ITSM ticket to CSSC Brunssum, technical support or via e-mail to the CSSC Resource Management Branch (RMB) who will coordinate internally to assess feasibility, required effort and personnel to be involved.

Service Flavors:

In-House support:

- TE and FOR will be maintained within the CSSC where additional shipping costs could arise.
- All devices to be TEMPEST tested need to be send to the CSSC.

On-Site support:

- Based on an accepted price proposal, TE and FOR will be maintained at customer location where additional transportation and staffing costs arise.

Available on: N/A

Service prerequisites:

- Operational Units have completed Level 1 and 2 maintenance activities including cleaning as laid down in the system maintenance guides.
- To ensure that battery operated TE are charged regularly.
- To provide access to any password protected hard drive.
- Operational Units have conducted a full inventory check of the system prior to the Handover Takeover (HO/TO) to the CSSC engineering and asset management teams to ensure that power supplies, batteries, and terminal connectors / adapters are included.
- Real Life Support provided at deployed locations to enable the conduct of the maintenance.

Underlying Services: OTH001

Standard Service support levels: N/A

Service Cost/ Price: The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Categorized areas of measurement capability and types supported. Due to the huge variety of different models and build-in options, detailed costs will be provided to customers on a case-by-case. Cost in TAS hours seen in table below, is indicative average cost per item.

	Type of Test Equipment	Support	Average Costs
Category A	RF attenuator set / step, termination, power splitter / divider, directional coupler, high power load, optical sources, power meter, attenuator, optical laser source, fusion splicer, cable analyser, smart remote, LAN tester, digital multimeter (hand held), clamp on meter, high voltage probe, ISDN tester, bit error rate tester, RF power sensor, sweep generator, frequency counter, radiation meter and field probe, 8,5 digit bench multimeter, oscilloscope (Hand Held), megger, cable tester, data communication analyser, media test set ...	TE In-house Onsite	Average TAS hours 1.5, which could deviate depending of the model to be tested.
Category B	OTDR modules, spectrum analyser (hand held), oscilloscope, earth ground tester, communication analyser, function generator, test set analyser...	TE In-house Onsite	Average TAS hours 3.0, which could deviate depending of the model and options installed.
Category C	RF signal generator, level generator, OTDR (hand held), ...	TE In-house Onsite	Average TAS hours 5.0, which could deviate depending of the model and options installed.
Category D	OTDR bench type (quad models), precision spectrum analyser, ATM tester, network analyser, signal analyser...	TE In-house Onsite	Average TAS hours 8.0, which could deviate depending of the model and options installed.
Category E	Repair of fibre optic cable reel and testing (e.g. 500m, Type HMA connector, Single Mode)	FOR In-house	Average TAS hours 3.0, which could deviate depending of the type, and installed connectors.

	Type of TEMPEST Equipment	Support	Average Costs
Category A	Keyboard, smartcard readers, ...	TEMPEST In-house	Average TAS hours 0.5, which could deviate depending of the model to be tested.

Category B	Ext. DVD writer, monitor, TFT, KVM, switch, router, VoIP Phone, tablet, firewall, ...	TEMPEST In-house	Average TAS hours 2.0, which could deviate depending of the model and options installed.
Category C	Server, scanner, PC, projector, Thin Client, beamer, printer, ...	TEMPEST In-house	Average TAS hours 2.5, which could deviate depending of the model and options installed.
Category D	Video Teleconference (VTC), Laptop ...	TEMPEST In-house	Average TAS hours 4.0, which could deviate depending of the model and options installed.

LOG003 Test and Evaluation of Electromagnetic Environmental Effects Service – 3rd Level

Service ID: LOG003

Service Name: Test and Evaluation of Electromagnetic Environmental Effects Service – 3rd Level

Portfolio Group: Logistic Services

Service Description: The Service entails Shielding Effectiveness Testing and maintenance of shielded enclosures to meet the requirements for Electromagnetic Pulse Protection (EMPP), Communication Security (COMSEC), TEMPEST and any other Radio Frequency (RF) interference protection on NATO common static facilities and transportable CIS systems according to MIL-STD-188 125-1/2 and SDIP 29/2. Testing is performed on all NATO shielded enclosures and bunkers, detailed in the ACO Directive 80-052 and all NATO mobile Communications and Information Systems (CIS) embedded in shelters or transportable boxes particularly used with CP0149 at various locations and mission related systems in Resolute Support (RS).

Value proposition: Regular inspections / maintenance are required to assure the required Radio Frequency (RF) shielding for all NATO common funded facilities, installations, and CIS (ACE Manual 93-5-1). Inspection serves the purpose to determine whether the facilities, installations and CIS are protected for EMP, COMSEC and TEMPEST. Testing, in accordance with the equivalent standards and the use of associated reference documentation, is the mandated method of managing the risk of damages caused by electromagnetic pulse and of avoiding the capturing and re-transmitting of NATO classified information.

Service Features:

- Planning, scheduling and coordination for electromagnetic environmental effects (E3) service
- Subject Matter Expertise (SME) in RF measurements of attenuation provided by the shield (Shielding Effectiveness [SE] testing) according to the IEEE STD-299, as well on existing and new up-coming projects with E3 concerns
- Testing of:
 - RF Shielded Enclosures
 - TEMPEST Testing Facilities
 - Microwave Sites
 - Satellite Ground Terminal (SGT)
 - Satellite Ground Segment (SGS)
 - CIS Systems (TSGT 2nd & TSGT 3rd Generation; SRDLOS; LRDLOS)
 - CIS Shelters (HF; Crypto; Helpdesk; AirC2; SIGINT COINS; NNCCRS)
- EMPP testing of Bunkers as detailed in the Allied Command Operation (ACO) Directive 80-5
- Annual inspection and preventive maintenance according to Allied Command Europe (ACE) Manual 93-5-1
- Testing of power and signal line filters according to MIL-STD-220 and publication method CISPR17

- Maintenance on manual and pneumatic operated electromagnetic shielded doors
- Acceptance testing of new and modified installations
- Technical advice of lightning, surge protection and grounding of CIS networks including power distribution systems
- Analysis and technical advice related to Electromagnetic Field Safety (EMF) of workplaces imposed by European and derived National Regulations

Service Flavors:

- **On-Site Support:** testing and measurements performed at the customer's site.

Available on: N/A

Service prerequisites: None

Underlying Services: OTH001

Standard Service support levels: N/A

Service Cost/ Price: Service Cost / Price: The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

LOG004 Inspection of Electronic Devices for Security Measures

Service ID: LOG004

Service Name: Inspection of electronic devices for security measures

Portfolio Group: Logistic Services

Service Description: The Service entails measurement of extremely low-level RF emanating signals of electrical devices. Within a shielded enclosure, isolated from external RF environmental noise, the RF energy of activated devices can be detected and reported across a wide frequency band. This could be used for individual devices, smaller than 80cm width, up to a system of components.

Value Proposition: Physical and technical inspection of equipment is essential to mitigate the threats associated with the unauthorized implantation of devices, substitution of equipment or manipulation of functionality within electronic equipment to achieve an eavesdropping capability. Without this initial inspection, electronic equipment is not readily possible to determine whether or not the equipment is “fit for purpose” and more importantly, whether or not it is “secure”. The level of security being directly correlated to whether or not such equipment contains any embedded malware and / or eavesdropping devices that can be exploited to capture and re-transmit NATO classified information.

Service Features:

- **Active testing technique:** undertaken by actively stimulating the equipment (i.e. simulating the processing of information).
- **Passive testing technique:** listening to the equipment’s electronic operation to detect any unusual or unexplained functionality, emanated signals and/or frequencies.
- **Shielded enclosure testing** for bugs, excessive Radio Frequencies (RF) emissions at frequencies around GSM 3G/4G and Wifi. Evaluation of Emanating Radiation (ER) for compromising emanation.
- **Analysis** of the effects of broadcasting audio signals
- **24h test** to look for transmissions of signals without any stimulus.

Service Flavors: The service is offered as a single flavour:

In-House support: all devices to be tested need to be send to the CSSC where additional shipping costs could arise.

Available on: N/A

Service Prerequisites: None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure is per testing. Provided the variety of possible device and enclosure testing, each testing is costed specifically.

LOG005 Support to Exercises with Deployable CIS Equipment Pool (DCEP) Service

Service ID: LOG005

Service Name: Support to Exercises with Deployable CIS Equipment Pool (DCEP) Service

Portfolio Group: Logistic Services

Service Description: The Service provides CIS user equipment from a DCEP Pool to eligible customers in order to support the exercise requirements of the Allied Command Operations (ACO). The service comprises: planning and coordination activities to make sure that high level exercise support requirements are matched with technical capability and existing capacity of DCEP; asset management and supply (including arranging transportation), maintenance (bench check, cleaning and serviceability testing) as well as logistics maintenance support of the DCEP pool.

The pool contains laptops, workstations, telephones, printers, projectors, Video Teleconference (VTC) Terminals, Multi-Function Devices (MFD), and LAN extension assets to expand the user access domains for each flavour of the DCIS node (in accordance with INF020 service definition).

The service does not comprise: build, upgrade, repair of DCEP pool assets (covered by INF020), on-site support and support to customer funded exercises (covered by specific Exercise Budget), upgrade (major configuration changes covered by NSIP projects). Costs of commercial shipments are charged against respective exercises.

Value Proposition: Centralization of the DCEP pool at CIS Sustainment Support Centre (CSSC) enabling smooth and coordinated CIS user equipment distribution to customers in support of the exercise requirements of the Allied Command Operations (ACO).

Service Features: Support to Exercises with Deployable CIS Equipment Pool (DCEP) Service provides planning and coordination, logistics as well as maintenance activities.

- **Planning and Coordination:** In coordination with NCIA Operations and Exercises Service Line (OPEX), appropriate CSSC representation is present at key planning events in order to provide right level expertise required to evaluate feasibility of requirements' fulfilment and coordination of proceedings leading to the provision of service at a required level. Resource Management Branch (RMB) leads this process. Upon receipt of the DCEP requirements, CSSC analyses them by performing quantitative and qualitative checks as well as, together with ACO J6 CyOC and NCISG, de-conflicting delivery dates for the customer locations. CSSC receives requirements from OPEX according to the timelines based on ACO exercise planning process. As in INF020 service, Service Delivery Schedule and Change Management Plan as planning and coordination tools are used and updated on a monthly basis. Service Delivery Managers (SDM) also provide Service Availability Management and Service Obsolescence Management Reports.

- **Logistics:**

o **Storage:** Most of DCEP assets are stored in sturdy cases allowing multiple deployments without too quick degradation of equipment. After DCEP is received back from exercise and cleaning, bench check test, serviceability check (maintenance activities) are accomplished, equipment is put back each time into cases making preparation time for next deployments shorter.

o **Dispatch:** After CSSC internal task is released, respective asset management activities are performed and the warehouse team (cleanliness, serviceability check), along with the crypto custodians as required, prepare consignments to be dispatched to the customer. Receipt and Dispatch (R&D) team coordinates and tracks deliveries, as per requested timelines. Equipment can be collected or shipped commercially, as per requirements/possibilities. Shipping is not included in the service rate.

o **Receipt:** Upon completion of the exercise, the DCEP is returned, in its entirety to the R&D and inventoried within 24 hours of physical receipt. As discrepancies are identified, the R&D reports the information to the RMB for rectification.

o **Logistics Maintenance Coordination (LMC):** Equipment returned from exercises is processed to respective workshops and according to particular types of equipment for serviceability test (e.g.: motherboard, memory, processor, network card, video card, storage, battery, usb).

• **Maintenance:** The various workshops of the Engineering and Maintenance Branch (EMB) perform full serviceability check of received equipment. After bench checking all serviceable assets are sent back to storage. If unserviceable items are identified, they will be processed for repair at CSSC or sent for an external repair. Note: The repair itself is excluded from this service as included in INF020.

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service Prerequisites: DCEP capability is provided by service INF020.

Underlying Services: OTH001

Standard Service Support Levels:

- **In House:** Equipment is stored, maintained and managed at the CSSC main warehouse and received and/or issued on request.
- **Routine:** Service provided as a routine process associated with standard timelines.
- **Urgent:** Service provided as a prioritized process associated with urgent requirements and time-lines.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

This page is left blank intentionally



Other Services

This page is left blank intentionally

OTH002 Account Management Service

Service ID: OTH002

Service Name: Account Management Service

Portfolio Group: Other Services

Service Description: The Account Management Service ensures that NCIA eligible customers and operational partners are supported through a structured account management framework. Account Managers act as a “trusted advisor”, being the principal interface between customers and the Agency’s organisational elements (Business Areas, CSUs, CSEs, etc.), establishing trusted relationships, capturing customer requirements, translating them into actionable IT service needs and representing Customers’ interest within the Agency.

This service is delivered under the framework of an established and signed service agreement and cannot be requested separately, i.e. outside of such an agreement.

Account Management is delivered through a **structured framework** that provides both strategic oversight and operational execution. The Account Manager (AM) plays a key role in long-term engagement, alignment between NCIA and Customer’s priorities, and ensuring consistency across customers. Where applicable, local CSU staff, in particular CSU Commanders, acting as the Service Management Authority (SMA), provide operational account support through day-to-day interactions, local follow-up, and customer relationship management. Both the AM and CSU contribute to the same set of account management activities (features) but from complementary perspectives, ensuring customers benefit from a holistic approach that balances strategic alignment with operational responsiveness.

Value Proposition: The Account Management Service offers customers a clear and accountable entry point into the Agency for the full range of CIS services and projects. It enables structured engagement, transparent and effective requirements capture, monitoring, and feedback, thereby enhancing NCIA responsiveness and aligning projects and services with customer objectives.

The Account Manager (AM) serves as the customer’s primary interface for service discussions, strategic engagement, and escalations, supported by local CSU staff who ensure continuity at the operational level. This combined approach provides consistency, fosters efficiencies, and ensures alignment across central and local roles.

Service Features

- **RFI Management:** Coordinating and delivering authoritative responses to customer Requests for Information (RFIs).
- **Risk Management:** Identifying, assessing, and monitoring risks to service and project delivery, or account engagement.
- **Support to CIS Budget Development and Follow-up:** Helping customers formulate requirements into budget submissions and tracking execution.

- **Demand Management:** Balancing customer needs with NCIA resources, ensuring prioritisation and feasibility.
- **Support to QSLR Process and Escalation Path:** Participation in and contribution to Quarterly Service Level Reviews (QSLRs) and supporting a structured escalation Process.
- **Business Intake - CRF Management, Project Status Follow-up:** Overseeing the lifecycle of Customer Request Forms (CRFs) and ensuring projects, including progress tracking and communication and supporting a structured escalation channel.
- **RFC Management:** Coordinating Requests for Change (RFCs) to existing services agreements, in line with Agency processes.
- **Strategic Alignment, Business Development, and Opportunity Management:** Ensuring services remain aligned with Customers' mission objectives and identifying opportunities for service improvement.
- **CRM and Customer Problem / Complaint Handling:** Providing a clear channel for handling issues, complaints, and problem resolution.
- **Contract and SLA Management:** Leading the negotiation, supporting development and execution, of contracts and Service Level Agreements.
- **Reporting and Communication:** Delivering structured reports, dashboards, and updates on service delivery and projects/CRF lifecycle to maintain transparency and informed decision-making.
- **Service Portfolio Awareness & Guidance:** keeping customers informed about the NCIA costed customer service catalogue, new offerings, and how they can be leveraged to meet Customers' mission objectives.

Service Flavours: The Service is available in following flavours:

Account Management of the Centralized Service Level Agreement (CSLA): provides AM service to a customer having a large, consolidated service level agreement with NCI Agency for provision of the Centralized / Backbone CIS services across entire NATO CIS enterprise. Applicable only to the Centralized Service Level Agreement.

Account Management of an Enterprise Service Level Agreement (ESLA): provides AM service to customer(s) having a consolidated service level agreement with NCI Agency for provision of CIS services to multiple user organizations customers tied into one organizational and/or budget structure.

Account Management of a Individual HQ Service Level Agreement (SLA): provides AM service to customers having a service agreement with NCI Agency for provision of CIS services to a single user organization (which may have elements of other user organizations as additional elements within the same SLA).

Account Management of a Service Support Package (SSP): provides AM service to customers having a Service Support Package with NCI Agency for provision of CIS services.

Available on: N/A

Service Prerequisites: Formal agreement

Standard Service Support Levels: N/A



Service Cost / Price: The unit of measure for the Service is Per Agreement. For the price details, see the Service Rates document.

OTH003 AirC2 In Service Support Program of Work (ISS POW) General Support Service

Service ID: OTH003

Service Name: AirC2 In Service Support Program of Work (ISS POW) General Support Service

Portfolio Group: Other Services

Service Description: The Service entails services provided to ACO as a part of the AirC2 ISS POW that are not directly related to individual application services, due to the generic nature of performed activities to support services across a number of systems.

Value proposition: The service enables the overall delivery of the in-service-support for a number of applications and systems in support of the NATO Integrated Air and Missile Defence System (NATINAMDS).

Service Features: The service entails the following activities:

- Contract and licence management;
- Interoperability management;
- Security management;
- Support to AirC2 governance meetings and related NATO committees and Working Groups;
- Support to enabling Platforms and Tools;
- Development of POW related price proposals and requirements documents.

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

OTH005 Training Capability Battle Lab Support Service

Service ID: OTH005

Service Name: Training Capability Battle Lab Support Service

Portfolio Group: Other Services

Service Description: The Training Capability Battle Lab Support Service provides CIS services^{*1} and expertise in the Modelling and Simulation (M&S), Training and Exercise (T&E), and CIS expertise required to support planning, design, management, and execution of the customer's Training Capability Battle Lab's annual program of work for testing, experimentation, capability development and wargaming in support of Warfare Development.

Caveats:

- The service assumes that the security accreditation and the operational use of the Training Capability Battle Lab are responsibilities of the customer.
- The service provides O&M of one unclassified platform.
- The service is currently designed for the JFTC environment and to meet JFTC's requirements.

^{*1} Disclaimer: The IT platform and services are provided locally and will need to be modified to be ITM compliant after ITM delivers to the sites where this platform is used.

Value Proposition: The service supports:

1. Testing, experimentation and concept development requirements based on a combination of existing and/or new M&S, T&E, and interoperable capabilities of NATO, Allies, Partner Nations, and Industry.
2. Wargaming requirements based on existing NATO Modelling and Simulation capabilities with validated data sets replicating multi-operational domain warfare environment.

Service Features:

The service provides the following:

1. Management of a platform, including a combination of existing and/or new M&S, T&E and interoperable capabilities of NATO on the Battle Lab Unclassified standalone platform with VPN connectivity.
2. A combination of existing and/or new T&E and/or interoperable capabilities of NATO on the following existing platforms:
 - CFBLNet Pink,
 - CFBLNet Grey,
 - Exercise MS.
3. Existing NATO T&E capabilities with support for validation of data sets replicating multi-operational domain warfare environment on the existing Exercise MS platform.
4. Best-effort CIS support on the existing Battle Lab Standalone unmanaged platform that consists of laptops with OS connected to a standalone LAN.

5. The required flexibility, enabled by providing:

- Standing capabilities on supported platforms with a pre-defined set of systems and their interconnections;
- Pro-active maintenance to prevent issues and manage availability;
- Managed roadmap for systems to ensure agreed versions of systems are available and operational;
- 10% capacity to add new capabilities or new versions of capabilities;
- Dedicated on-site support by a team of CIS staff integrated with the customers' Battle Lab event management team;
- A set of pre-approved standard service requests with defined standard service fulfilment times;
- Critical priority response and restoration times (P1) during Training Capability Battle Lab event execution or as agreed in the event planning phase;
- Remote connections for remote support purposes;
- Remote connections for 3rd party users;
- Provisions for on-boarding of non-AFPL listed systems and users.

Service Flavours: The Service is available as a single flavour.

Available on: NU Standalone, MS (Exercise NS), CFBLNet Pink, CFBLNet Gray

Service Prerequisites: This service is a combination of SME services and locally provided CIS services on the existing platforms, limited to MS, CFBLNet networks, and Battle Lab Unclassified Standalone. In principle, the locally provided services are provided based on (where available) or in line with the existing services provided by NCI Agency. The service assumes that the required target platforms are not part of the service and that they are already available.

Standard Service Support Levels:

Service Time Window	Priority
Planned event execution • pre-approved service requests	P1 – Critical During business hours in working days
Planned event execution • other service requests	P3 During business hours in working days
Regular (outside planned events), including event planning, preparation and tear-down	P3 During business hours in working days

Service Availability Target:

- Downtimes for maintenance - number of allowed downtimes: 1 per month, pre-notification periods: 2 weeks, max downtime time pre system: 2 working days

- Maximum service usage time without maintenance: 1 month
- Interruptions to the Service (both planned and unplanned) will be coordinated with the Customers' Battle Lab manager

Service Restoration:

Priority	Time to Respond (Incident or Service Request)	Time to Restore (Incidents)
P1 – Critical During business hours in working days	1 h wall clock	4 h wall clock
P3 During business hours in working days	8 h business hours or 1 working day	16 Business hours or 2 working days

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.



Training Services

TRA003 Education and Individual Training Availability and Maintenance (EIT A&M)

Service ID: TRA003

Service Name: Education and Individual Training Availability and Maintenance

Portfolio Group: Training services

Service Description: This service maintains the NATO-Required training curriculum delivered through service TRA002: Education and Individual Training Delivery and ensures the availability of professional, certified instructional capacity and the high quality training capability to plan, coordinate and deliver these courses.

Value Proposition: This service mitigates the operational risk to customers that NATO-Required courses are discontinued by the NCI Agency as a result of not breaking even on course prices and ensures that NCS elements have seat allocation priority on those courses. The service reduces the volatility of the course prices and increases the predictability of the annual customer budgets required for Education and Individual Training.

Service Features: N/A

Service Flavours: N/A

Available on: N/A

Service Prerequisites: Maintenance of training systems, including underlying hardware, software and applications, SME and Security Services, on which the Education and Individual Training courses are provided. The operation and maintenance of the Academy Learning Environment (ALE) which includes specialist IT, training management systems, and Learning Management System (JADL) used for on-site, live on-line, self-paced, and blended learning delivery by TRA002 and other services. The development of courses funded by NSIP or Programmes of Work (PoWs).

Standard Service Support Levels:

Service Availability¹ Target: N/A

Service Restoration: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.



NATO HQ Only Services

WPS001N NHQ Managed Device Service

Service ID: WPS001N

Service Name: NHQ Managed Device Service

Service Type: Customer Facing

Portfolio Group: NATO Digital Workplace Services

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NHQ Managed Device Service provides end users with a client device (of various form factors) that enables secure access to NATO HQ networks. The service includes the Windows operating system, Microsoft Office Professional Suite, NATO-mandated security tools, and other baseline software. Services for cloud-based devices are out of scope.

Value Proposition

This service ensures operational efficiency by delivering a standardized and secure managed device that connects to NATO HQ CIS resources. It supports access to office automation, internal applications, browsing, and other mission-critical functions throughout NATO HQ.

Service Features

- Windows OS with baseline software and configuration
- Microsoft Office Professional Suite
- Required NATO HQ security tools
- Controlled access to peripherals
- Support for applications included in the base-image including packaging, patching, and deployment.
- Includes Level 1 & 2 Support
- Excludes hardware procurement.

Compliance & Baseline Management

- All managed devices are configured and maintained in accordance with NATO HQ compliance policies and operational baselines.
- Mandatory security patching is enforced through centrally managed update processes.
- Devices must remain compliant with the standard NATO HQ baseline; unauthorized modifications are not supported.
- Compliance audits and reporting are performed periodically, including during QSLR meetings.
- Any deviation from the baseline requires formal approval through Change Management processes.

Service Ordering and Request

NATO HQ IS / IMS Customers
Devices are requested via ITSM tickets. Hardware is deployed from pre-purchased stock. If stock is unavailable, acquisition is handled via new project or SVP.

Agencies and Delegations
Devices are requested via CRF. In-service support is governed by annual Service Agreements.

For all users, the NATO HQ Service Centre is the Single Point of Contact (SPOC) for incidents and service requests.

Service Flavours

WPS001N-A: Thick Client (Static Desktop / Workstation)

- Requires wired network connection
- Includes monitor (min. 24"), keyboard, mouse
- Optional (stock-dependent): second monitor, VTC camera, headset, KVM

WPS001N-B: Thin Client Device

- Optimized for remote server environments
- Includes monitor (min. 24"), keyboard, mouse
- Optional (stock-dependent): second monitor, VTC camera, headset, KVM

WPS001N-C: Portable (Laptop/Tablet) Device

- Supports wired and wireless connections
- Laptop includes:
 - Bag
 - DELL USB-C to USB-A/HDMI Adapter
 - USB-C to USB-A adapter
 - DELL A/C Adaptor 100W
 - Kensington Privacy screen and its protective cover
 - Headset.

N.B : Keyboard Ratio QWERTY / AZERTY : 80/20

Available on

Thick Client:

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

Thin Client:

- ATHENA (N950)
- MAGELLAN (R950)

Portable Device:

- MAGELLAN (R950)

Service Prerequisites

- INF001N
- INF004N
- WPS002N
- OTH001N

Underlying Services

N/A

Standard Service Support Levels

- **Availability Target:** 99.0%
- **Standard Delivery Time:** 3 working days for installation and configuration
- **Service Restoration (P0/P1):** 4 hours



N.B. Resolution times and service priorities follow NCI Agency SLA, SSP, or other formal agreements.

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Service Cost / Price

- **Service Unit:** Per device

Device	Unit
Thick Client	1
Thin Client	1
Portable (Laptop/Tablet)	1

WPS002N NHQ Identity Access Management Service

Service ID: WPS002N

Service Name: NHQ Identity Access Management Service

Service Type: Supporting

Portfolio Group: Workplace Services

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NHQ Identity Access Management Service provides identities (including provisioning and de-provisioning of User Accounts, Privileged Accounts, Service Accounts, Computer Accounts), and the capability to share trusted identity information between different domains and to NHQ users. The information on identities retrieved from different authoritative sources.

The Service allows controlled access based services. The access services can be available across domains utilizing AD-Federation. It offers a Single Sign On experience for users with a valid NATO HQ Identity.

The Management of the infrastructure supporting this Service is included in INF004N. The infrastructure and licensing supporting the Smart Cards is included in SEC015N.

This service also includes the provision of an office relocation function for the support of ICT aspects during staff moves. Up to five staff moves are included per working week.

Value Proposition

This service ensures secure, efficient, and policy-compliant management of digital identities and access rights across NATO HQ CIS environments. It supports the full identity lifecycle — from on-boarding and role-based access provisioning to deactivation — while enforcing strict access control and auditability aligned with NATO security policies.

As part of office moves or organizational restructuring, the service ensures seamless continuity of access, minimizing downtime and operational risk. Users are provisioned into their new roles and locations with the appropriate permissions, ensuring mission readiness and compliance.

Service Features

- **Identity Management**
 - Shared information across multiple identity stores, improving data quality and reducing overhead for connected systems. Identity information can be synchronized between different affiliates, supported by automated workflows and enables account provisioning and de-provisioning. The Lifecycle management (from provisioning to de-provisioning) of Identity and its attributes is being provided.
- **Access Management**
 - Is available for the compatible services requiring authentication for users and/or resources. The access management (authentication/control/validation) is provided by credential management, security group memberships, and policies (like GPO), also through integration with NATO PKI.
- **Office Move Support**
 - Seamless migration of user accounts and access rights during office relocations or restructuring.
 - Pre-move planning and coordination is required to ensure minimal operational disruption.

Service Ordering and Request

- **NATO HQ IM / IMS Customers**
 - Accounts are requested via ITSM tickets.
- **Agencies and Delegations**
 - Accounts are requested via CRF
- **Office Moves**
 - Should more than 5 moves per week be required, an impact assessment will be made and a proposal provided to the IS and/or IMS to carry out the necessary moves with Contractor Support. Where no ICT implication is involved for staff moves, this restriction on moves does not apply.



For all users, the NATO HQ Service Centre is the Single Point of Contact (SPOC) for incidents and service requests.

Service Flavours

The Service is available as a single flavour which is costed per account.

Available on

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

Service Prerequisites

- INF001N
- INF004N
- WPS001N
- WPS003N
- SEC015N
- OTH001N

Underlying Services

N/A

Standard Service Support Levels

User Account Creation Time after account is created in NHQ IDams system: < 5 Days.

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

- **Service Unit:** 1 Account
- **N.B.:** If a single person requires accounts on 3 different NHQ CIS this would count as a quantity of 3

WPS009N NHQ Voice and E-mail Service

Service ID: WPS009N

Service Name: NHQ Voice and E-mail Service

Service Type: Supporting

Portfolio Group: Workplace Services

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NHQ Voice and E-mail Service provides the ability to collaborate and communicate in real time and using E-mail on the clients included in WPS001N and the physical fixed phones at NATO HQ.

Value Proposition

The Service empowers the NHQ with dependable communication for voice, IM, video and E-mail. It enhances collaboration across teams and locations.

Service Features

- **Athena Skype Clients**
 - Communication up to NS for internal users
 - E-mail
 - Instant messaging

- Video when approved
- **Magellan Skype Clients**
 - Communication up to
 - NR for internal users
 - NU for external
 - E-mail
 - Instant messaging
 - Voice
 - Video
- **Desk-phones**
 - Voice communication up to NU
 - Internal
 - External when authorized
- **Public phones** (corridor/elevator)
 - Voice communication up to NU
 - Internal

Service Ordering and Request

- **NATO HQ IM / IMS Customers**
Devices are requested via ITSM tickets. Hardware is deployed from pre-purchased stock. If stock is unavailable, acquisition is handled via new project or SVP.
- **Agencies and Delegations**
Devices are requested via CRF. In-service support is governed by annual Service Agreements.

For all users, the NATO HQ Service Centre is the Single Point of Contact (SPOC) for incidents and service requests.

N.B. The procurement of software and hardware (including end-user devices) and lifecycle replacement is excluded from the service support cost (O&M) and must be procured separately.

Service Flavours

The Service is available in following flavours :

- **Skype and E-mail:**
A unified communication option combining Skype voice services with corporate e-mail capabilities.
- **Physical phone:**
A physical device installed in offices or public areas at NHQ for voice communication. Relying on a network connection as opposed to a mobile device.

Available on

- **Static Desk Phone:**
 - NATO HQ Voice Network

- Highest content classification: UNCLASSIFIED
- **Softphone (Skype for Business):**
 - Magellan Clients
 - Athena Clients

Service Prerequisites

- INF001N
- LEG008301 PBX
- OTH001N

Underlying Services

N/A

Standard Service Support Levels

Support Window	Availability Target	Restoration Time (P0/P1)
During Support Hours	99.9%	1 hour
Outside Support Hours	99.5%	4 hours

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

Flavour	Unit
Static Desk phone	1
Skype / E-mail	1

N.B.: If a single person requires Skype accounts on 2 different NHQ CIS this would count as a quantity of 2.

WPS016N NHQ Managed Mobility Service

Service ID: WPS016N

Service Name: NHQ Managed Mobility Service

Service Type: Supporting

Portfolio Group: Workplace Services

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NHQ Managed Mobility Service provides the users with a fully managed mobility solution enabling users to connect to NATO HQ Restricted network. It includes the capability to connect a managed Apple iOS device (Smartphone or Tablet) to NATO HQ Restricted services such as e-mail and other NHQ business applications.

Value Proposition

The Service offers a single customer experience when accessing NATO HQ network from authorised Apple iOS smartphone and tablet devices. The service allows for better availability of end-users and fast reaction to critical action items while being distant from the office.

The procurement of the hardware and lifecycle replacement is excluded from the service cost and must be paid separately.

Service Features

The service provides mobile users with the capability to access NHQ Applications and mobile apps, in line with NATO security requirements.

In detail, the Service features are:

- Managed device in accordance with the NATO HQ security guidelines;
- Mobile subscription, cellular provider expense management, and data cost management;
- Productivity mobile apps (e.g. mail app, collaboration apps, web browser).
- A GSM relay capability to ensure public GSM signals propagate inside the NHQ building.

Service Ordering and Request

- **NATO HQ IS / IMS Customers**
Devices are requested via ITSM tickets. Hardware is deployed from pre-purchased stock. If stock is unavailable, acquisition is handled via new project or SVP.
- **Agencies and Delegations**
Devices are requested via CRF. In-service support is governed by annual Service Agreements.

For all users, the NATO HQ Service Centre is the Single Point of Contact (SPOC) for incidents and service requests.

Service Flavours

The Service is available at two options WPS016N-1 GSM Relay, non unitized. WPS016N-3 MDM, per 1 unit.

Service options (additional charges apply):
The Mobile Secure Communication option is available for these devices, but is ordered separately using the NCIA Enterprise WPS016-E Mobile Secure Communication (SecuSuite)

Available on

- Magellan (R950)

Service Prerequisites

- INF001N
- INF004N
- OTH001N

Underlying Services

N/A

Standard Service Support Levels



Support Window	Availability Target	Restoration Time (P0/P1)
During Support Hours	99.9%	1 hour
Outside Support Hours	99.5%	4 hours

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

- **Service Unit:** 1 device

INF001N NHQ Local Area Network (LAN) Service

Service ID: INF001N

Service Name: NHQ Local Area Network (LAN) Service

Service Type: Customer Facing

Portfolio Group: Infrastructure Service

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NHQ LAN Service delivers secure and structured local network connectivity to NATO users on the NHQ campus, supporting wired and wireless access to designated NATO security domains.

The service is designed with modularity, scalability, and security in mind, aligning with NCI Agency service design principles. It integrates with other enabling services and supports continuous improvements via performance monitoring, capacity planning, and feedback loops.

Value Proposition

The NHQ LAN Service provides the foundation for accessing mission-critical services, collaboration platforms, and shared data within NATO HQ. It enables secure communication, fosters flexibility with mobile access, and ensures compliance with NATO security standards.

The Service is a key enabler for:

- Voice and Video Services
- Internet and Intranet Access
- Security and Management Services
- Seamless integration with Customer-Facing Services

Service Features

- Wired and wireless access across NATO HQ security domains
- Security enforcement via Network Access Control (NAC)
- Real-time monitoring and incident detection
- Capacity planning to match user and device footprint
- Integration with existing infrastructure and service layers
- Service design aligned with ITIL and NATO HQ service management practices
- All endpoints connecting to the LAN are subject to policy-based access control
- Dynamic VLAN assignment based on role, device type, and authentication
- Network traffic monitoring using NATO-approved tools
- Detection of anomalous behavior and unauthorized access attempts
- Event logging for compliance and forensic analysis
- Modular design allows future enhancements without disrupting current operations
- Service metrics and KPIs monitored to ensure performance and reliability
- Integration with CMDB for asset tracking and change management
- Security patching and product upgrades.
- Includes Level 2 & 3 Support
- Excludes physical cabling (managed by NHQ IFM)

Service Ordering and Request

Service requests are initiated through the NHQ Service Request Portal on the Intranet.

Incident and support requests follow standard support workflows.

Service Flavours

- **Wired LAN**

For fixed workstations and devices; available on:

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

- **Wireless LAN**

For mobile devices; available on:

- PUBLIC (U950)

Service Prerequisites

- OTH001N
- SEC007N
- Existing building cabling managed by NHQ IFM

Underlying Services

N/A

Standard Service Support Levels

Support Window	Availability Target	Restoration Time (P0/P1)
During Support Hours	99.9%	1 hour
Outside Support Hours	99.5%	4 hours

N.B. Full Priority Resolution Times and the Generic Service Priority Assignment Matrix will be followed per NCI Agency NHQ SLA.

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training (Not Included in Service Cost)

N/A

Service Cost / Price

- **Service Unit:** Per port
- Estimated as :

$\text{Rate/1 port} \times (\# \text{Laptop} + \# \text{Thick} + \# \text{Thin} + 75\% \# \text{phones}) \times 2$

INF004N NHQ Infrastructure as a Service

Service ID: INF004N

Service Name: NHQ Infrastructure as a Service

Service Type: Supporting

Portfolio Group: Infrastructure Service

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NHQ IaaS is a flexible, scalable and redundant Infrastructure offering. It provides Core Services (Active Directory, DNS, DHCP, etc.), Processing & Storage and Back-up/Restore capabilities to host Virtual Machines, Databases, Applications, and other services running on top of the operating systems to meet Customer's requirements. It excludes Network Infrastructure which is covered by INF001N.

Value Proposition

The NHQ Infrastructure as a Service (IaaS) offering provides a comprehensive and scalable solution designed to meet the organization's evolving IT needs. This service includes a range of essential components such as processing power and storage, a virtualization

platform, data storage, backup and restore capabilities, and core services like Active Directory (AD), DNS, and DHCP. Additionally, it encompasses other critical services that ensure the smooth operation and management of the NHQ IT infrastructure. By leveraging our IaaS, NATO HQ can efficiently manage its resources, enhance data protection, and maintain high performance and reliability.

Service Features

The IaaS offers the user the following:

- Scalability and Flexibility
- High Performance and Reliability
- Business Continuity Exercises
- Business Continuity Services (BCP2 / BCP4)
- Comprehensive Core Services
- Robust Data Protection
- Cost Efficiency
- Expert Support and Management
- Enhanced Security.

Service Flavours

The Service is available as a single flavour with a unit cost of 1.

Available on

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

N.B: IaaS for NHQ Cloud based Services are included in the cost of the Cloud Service and are not part of this Service.

Service Prerequisites

- INF001N
- OTH001N
- PLT006N

Underlying Services

N/A

Standard Service Support Levels

- **Availability & Restoration Targets:**

Built-in High Availability provides uniform failover protection against hardware and operating system outages.

Support Window	Availability Target	Restoration Time (P0/P1)
During Support Hours	99.9%	1 hour
Outside Support Hours	99.5%	4 hours

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

- **Service Unit: 1**

PLT006N NHQ Database Platform Service

Service ID: PLT006N

Service Name: NHQ Database Platform Service

Service Type: Supporting

Portfolio Group: Platform Service

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description:

The NHQ Database Platform Service provides a fully managed database platform for use as an integral part of a production, testing, staging, and/or development environment. The service provides flexible, scalable, and demand based platform, which is oriented toward central monitoring and management where underlying complexities of Database technologies (Oracle, MS SQL, and PostgreSQL) are encapsulated as a combined generic service.

Value Proposition:

The Service offers the following benefits:

- Lowered Total Cost of Ownership of a database through the provision of a consolidated, standardized and volume managed database environment;
- Agility to meet NATO HQ demands through provision of standardized, tested environments;

- Size and growth of a database monitored and provision of required capacity made to ensure continued availability and performance to meet operational needs;
- For standard use, the underlying technical complexities are isolated from the customers, technology agnostic;
- Increased security and availability through a dedicated team of experts who monitor the service

Service Features:

The NHQ Database Platform Service offers the user the following features:

- Database hardware capacity;
- Lifecycle management of the Database Platform;
- Database software licensing and maintenance;
- Fully managed
- Automated backup with point-in-time recovery;
- Software Lifecycle management including maintenance, upgrading and patching
- Level 2 & 3 Support;
- Database and performance monitoring and tuning;
- Capacity provisioning through scalable and flexible management of available resources.
- License management for the supported Database Types

Service Ordering and Request

Service requests are initiated through the NHQ Service Request Portal on the Intranet. Incident and support requests follow standard support workflows.

Service Flavours:

The NHQ Database Platform Service is available as a single flavour at the unit cost of 1.

Available on:

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

Service Prerequisites:

- INF001N
- INF004N
- OTH001N

Standard Service Support Levels:

- **Service Availability Target:**
Built-in High Availability provides uniform failover protection against hardware and operating system outages.

Support Window	Availability Target	Restoration Time (P0/P1)
During Support Hours	99.9%	1 hour
Outside Support Hours	99.5%	4 hours

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost::

N/A

Service Cost / Price:

- Service Unit: 1

APP001N NHQ COTS Applications

Service ID: APP001N

Service Name: NHQ COTS Applications

Service Type: Enabling

Portfolio Group: Application Services

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

This service offering is for the provisioning of Commercial-off-the-shelf (COTS) software licenses and software support renewals. The products requested must be approved by NHQ Program Management Office (PMO).

The purchase of Licenses is performed by Enterprise Configuration Asset Management (ECAM) aligned with the APP001 Service.

The difference between APP001 & APP001N is that the latter includes Cost to provide O&M Support including installation, upgrading and troubleshooting of the software

Value Proposition

The NHQ COTS Applications Service provides a reliable, secure, and field-proven software solutions that meet the NHQ's operational, security, and interoperability requirements. By leveraging commercially available applications, we enable faster deployment, reduced lifecycle costs, and enhanced mission readiness, while ensuring strict adherence to NHQ standards and regulations.

Through expert integration, continuous support, and proactive lifecycle management, we deliver resilient and scalable solutions that empower NHQ to operate more efficiently, collaborate more effectively, and respond rapidly to emerging challenges — strengthening collective defence and mission success.

Service Features

- Secure Deployment
- Interoperability
- Rapid Provisioning
- Lifecycle Management
- Configuration Management
- Standardized Cost.

Compliance & Baseline Management

N/A

Service Ordering and Request

The Service is available as a quantity of 1, with the specific details included in the NHQ SLA.

Service Flavours

The Service is available as a single flavour.

Available on

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

Service Prerequisites

- WPS001N

Underlying Services

N/A

Standard Service Support Levels



N/A

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Service Cost / Price

The costs for these products under this service are for both the license procurement and manpower support to package/install/maintain the application.

SEC001N NHQ Security Accreditation Support Service

Service ID: SEC001N

Service Name: NHQ Security Accreditation Support Service

Service Type: Supporting

Portfolio Group: Security Services

Status: Available

Service Background:

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description:

The NHQ Security Accreditation Support Service coordinates for security accreditation and re-accreditation activities for CSU Brussels owned services. It also provides guidance to staff working on other accreditation activities at NHQ.

Value Proposition:

This service documents and manages the security risk to the NATO HQ CIS, ensuring Cyber Security controls and mechanisms, are coherent and effective. Additionally it provides assurance and stability of a well understood regulatory framework by all stakeholders.

Service Features:

Security Accreditation Support Service is comprised of the following elements:

- **Security Accreditation Preparation and Documentation (New Systems):** Development of Security Accreditation Plan (SAP) together with project manager and obtaining approval to proceed from relevant Security Accreditation Authority (SAA). Working together with project team on development of security accreditation package (usually CIS description, Security Risk Assessment, Security Requirement Statement, Security Operating Procedures and Security Test and Verification Plan and Security and Verification Test Report) for new systems. Providing guidance and assistance to project team. Review of security accreditation package developed by project team. Coordination with relevant NATO Security Accreditation Authorities during project life cycle. Serves as first Point-of-Contact for Accreditation of new systems. This service feature is only available to and funded by projects that deliver new NATO HQ CIS that require accreditation.
- **Security Accreditation Support (In-service systems):** Provision of cyber security technical and policy support to Operational Commands and CIS Operating Authorities to manage risks and assist in the continued security accreditation of their CIS. Working together with System Managers and CIS Security Officers on updating of security accreditation package (usually CIS description, Security Risk Assessment, Security Requirement Statement, Security Operating Procedures and Security Test and Verification Plan and Security and Verification Test Report) for re-accreditation of systems in service. Providing guidance and assistance to System Managers and their team. Review of security accreditation package during CIS re-accreditation process. Comprehensive coordination with the NATO CIS Security Accreditation Board (NSAB) or any applicable Security Accreditation Authority (SAA). Guidance and support on security accreditation and re-accreditation activities as required by the NATO SAA's. Support for development of security accreditation strategies. Serves as first Point of Contact for re-accreditation of in-service systems.
- **Coordination in Security Risk Assessment Working Groups:** Support, lead, or coordinate Security Risk Assessment Working Groups for NATO HQ programmes or projects. This includes lead or coordinating the meetings and ex-committee work, providing advice regarding security risk assessment and risk management process, and support conducting SRA by the Group.

Service Flavours:

The Service is available as a single flavour at the unit cost of 1.

N.B: In general the CSU Brussels staff will be able to support the accreditation work for smaller projects. If there are issues providing support to small projects by the CSU this will be raised using the CIS Governance NHQ Portfolio Management Office. For all large projects the accreditation support will be funded separately by the project.

Service Available on:

- PUBLIC (U950)



- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

Service Prerequisites:

- OTH001N

Underlying Services:

N/A

Standard Service Support Levels:

N/A

Service Cost / Price:

Service Unit is 1.

SEC006N NHQ Cyber Security Incident Coordination Service

Service ID: SEC006N

Service Name: NHQ Cyber Security Incident Coordination Service

Service Type: Supporting

Portfolio Group: Security Services

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NATO HQ Cyber Security Incident Coordination Service connects the different stakeholders involved in NHQ cyber security incidents together in a structured and efficient way. These stakeholders include the different technical teams in CSU Brussels, NCSC, ICTM and NOS within the agreed frameworks.

Value Proposition

This service coordinates Incident Handling and Response at NATO HQ. The experienced, effective and efficient management of identified incidents through the Cyber Security Incident Coordination Service ensure correct handling through incident lifecycle, in turn strengthening cyber security capability and therefore the overall effectiveness and productivity of the organisation.

Service Features:

The Service covers the entire cyber incident response life cycle:

- Preparation;
- Identification;
- Containment;
- Eradication;
- Recovery;
- Lessons Learned

The Service also includes Alerting and Reporting

Service Ordering and Request

N/A

Service Flavours

The Service is available as a single flavour at a unit cost of 1.

Service Available on

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

Service Prerequisites

- INF001N
- INF004N
- OTH001N
- SEC007N
- SEC011N
- SEC012N

Underlying Services

N/A

Standard Service support levels

Support Window	Restoration Time (P0/P1)
During Support Hours	1 hour
Outside Support Hours	4 hours

Service Reporting



Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

- **Service Unit 1**

SEC007N NHQ Cyber Security Logging & Monitoring Service

Service ID: SEC007N

Service Name: NHQ Cyber Security Logging & Monitoring Service

Service Type: Supporting

Portfolio Group: Security Services

Service Status: Available

Service Background:

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description:

The NHQ Cyber Security Logging & Monitoring Service enables the collection and retention of security events at NHQ into centralized systems. As well as the monitoring and review of those events to detect security incidents.

Value Proposition:

This service enables early threat detection, fast incident response, and long-term cybersecurity improvement. By continuously capturing and analysing system activity, it helps protect critical assets, support compliance, and reduce operational risk.

Crucially, it provides detailed data for post-incident analysis—allowing teams to investigate security events, identify root causes, and implement preventive measures to strengthen future defences.

The Service fulfils the log-retention policy requirements for NATO HQ.

Service Features:

This service is comprised of the following elements:

- **Active Log Monitoring:**
Near Real-time monitoring and review of NHQ security logs to detect Cyber Security incidents. This feature is performed by NCSC resources using the SEC007N Service with funding included.
- **Security Information and Event Management System (SIEM) at NHQ**
This feature will perform the O&M for the logging platform on the Athena and Magellan Networks at NHQ
- **Collection of Logging Events at NHQ**
Maintaining the connection between the Log Sources at the NHQ and the Log Platform at NHQ.
- **Log Forwarding to Enterprise SIEM**
Configuring the NHQ Systems to forward the appropriate security logs to the NCSC managed Enterprise SIEM.

N.B.: This Service has the capability to maintain the settings and configurations for existing Log Sources at NHQ. Any new Log Sources that are introduced will need to provide additional funding to be integrated in this service.

Service Flavours:

The Service is available as a single flavour at the unit cost of 1.

Service Available on:

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

Service Prerequisites:

- INF001N
- INF004N
- OTH001N

Underlying Services:

- SEC007



Standard Service Support Levels:

Support Window	Availability Target	Restoration Time (P0/P1)
During Support Hours	99.9%	1 hour
Outside Support Hours	99.5%	4 hours

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price:

- Service Unit: 1

SEC011N NHQ Gateway Security Service

Service ID: SEC011N

Service Name: NHQ Gateway Security Service

Service Type: Supporting

Portfolio Group: Security Services

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NHQ Gateway Security Service provides a secure interconnection of different networks or network sections in order to protect the NATO HQ's key information.

The Service consists of the following technical components: Data Diodes, Firewalls, FileGuards, EmailGuards (including Email DLP), Web Proxies, Network DLP and VPN.

Value Proposition

The NHQ Security Gateway Service safeguards the controlled exchange of information between independent CIS environments or network segments, ensuring confidentiality, integrity and compliance with NATO Security Policies.

The service prevents unauthorized data flows, mitigates cyber threats, and minimizes the risk of data leakage or compromise.

Service Features

This service is comprised of the following elements:

- **Common to all:**
 - High Availability
 - Configuration Backup
 - Log forwarding to central repositories
 - Maintenance of system software
 - Health and availability monitoring
 - Device troubleshooting
 - Documentation
 - Development of SOP for repetitive activities (level 1, limited level 2)
 - Audit, accounting, authorization
 - Incident management, troubleshooting
 - Includes Level 2 & 3 Support
 - Security Incident Management support
 - Device management (bi-annual software update, weekly security content updates, emergency updates)
 - System specific policy management (following ITSM requests)
- **Gateway Security – Firewall Services:**
 - Support of physical, virtual and cloud-based firewalls
 - VPN support (Site-to-Site VPN)
 - Firewall rule review and validation, removal of unused/no longer required rules
 - Application of the incident response activities (blocking hosts, disconnecting networks, NIMBLs)
 - Development of custom application signatures
 - Testing/evaluation of new features and capabilities
 - Post deployment network adaptations and expansion (SRTS)
- **Gateway Security – VPN Services:**
 - Support of physical and virtual VPN
 - VPN support (Client/SSL VPN)
 - VPN rule review and validation, removal of unused/no longer required rules
 - Security Incident Management support
 - Application of the incident response activities (blocking hosts, disconnecting networks, NIMBLs)
 - Testing/evaluation of new features and capabilities
 - Network Access Control configuration for the Client VPN
 - Access configuration for Client VPN
- **Gateway Security – FileGuard Services:**
 - Support of physical FileGuards
 - FileGuards rule review and validation, removal of unused/no longer required rules
 - Security Incident Management support

- Application of the incident response activities (file types, file content)
- Testing/evaluation of new features and capabilities
- Configuration of flows
- Adaptation of release markings
- **Gateway Security – Data Diode Services:**
 - Support of physical Data Diode
 - Testing/evaluation of new features and capabilities
 - Configuration of new flows (SMB)
 - Configuration of new email domains
- **Gateway Security – Web Proxy Services:**
 - Support of physical, virtual and cloud-based web proxies
 - Web proxy rule review and validation, removal of unused/no longer required rules
 - Application of the incident response activities (blocking hosts, disconnecting networks, NIMBLs)
 - Testing/evaluation of new features and capabilities
- **Gateway Security – Network DLP Services:**
 - Support of physical and virtual network DLP
 - Network DLP rule review and recertification, removal of unused/no longer required rules
 - Application of the incident response activities (file types, file content)
 - Testing/evaluation of new features and capabilities
 - Adaptation of release markings

Service Flavours

Gateway Security Services NHQ comprise of the following flavours:

Flavour	Description
CDGW01	Interconnection between Athena NS and NS WAN
CDGW02	Interconnection between Magellan NR and NU WAN
CDGW03	Interconnection between NHQ Public and BT Internet
CDGW04	Interconnection between Athena NS and Partner Secret Network
CDGW05	Interconnection between Magellan NR and Athena NS
CDGWESS 952	Interconnection between Magellan NR and ESS
CDGW07	Interconnection between Magellan NR and NR WAN
CDGWESS 955	Interconnection between Magellan NR and ESS/MWB

CDGW09	NR VPN
CDGW11	Interconnection between BCP NS and NS WAN
CDGW12	Interconnection between BCP NR and NR WAN
CDGW NASO	Interconnection between Magellan NR and NASO Sites

Details about each Cross Domain Gateway (CDGW) are available in the corresponding NATO HQ CIS description document.

Available on

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

Service Prerequisites

- INF001N
- SEC007N
- OTH001N

Underlying Services

N/A

Standard Service Support Levels

Support Window	Availability Target	Restoration Time (P0/P1)
During Support Hours	99.9%	1 hour
Outside Support Hours	99.5%	4 hours

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

- Service Unit: 1

SEC012N NHQ CIS Endpoint Protection Support Service

Service ID: SEC012N

Service Name: NHQ CIS Endpoint Protection Support Service

Service Type: Supporting

Portfolio Group: Security Services

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NHQ CIS Endpoint Protection Support Service provides operations and management of the Endpoint Security Systems for the end-user devices and servers at NHQ.

The Endpoint security guidance consists of the following mandatory/optional controls, as per C3B Technical and Implementation Directive on CIS Security (AC/322-D/0048-REV3), as required by the NATO Office of Security;

- Endpoint antimalware
- Host-based Intrusion Prevention (IPS)
- Secure web-browsing
- Desktop Firewall
- Application whitelisting
- Central management control for Endpoint management
- Removable media protection

- USB Device Control protection
- Data-in-use Leakage Prevention
- Data-at-rest encryption
- Email antimalware

Value Proposition

The NHQ Endpoint Security Service provides centralized protection and management of end-user devices included in WPS001N as well as the servers from INF004N. It is designed to detect, prevent, and respond to cyber threats targeting Endpoint devices, helping to maintain the security, integrity, and compliance of the NHQ IT environment. The Service supports both on-site and remote users, ensuring consistent security policies and visibility across all Endpoints.

Service Features

The operations and management of NATO HQ Endpoint security software including:

- Full life cycle management for the respective Endpoint security controls.
- Reviewing and adapting the recommended Enterprise configuration and guidance for the NHQ requirements.
- Reviewing and adapting the recommended configuration and guidance for every new minor and major release.
- Monitoring the threat landscape for emerging threats and provide mitigation at Endpoint protection level.
- Providing Level 2 & 3 technical support
- Assisting with vulnerability remediation, as suggested by local CIS Security Officers or revealed from a vulnerability assessment.

Service Ordering and Request

The Service is linked to the ordering of EUD and servers.

Service Flavours

The Service is available at two flavours. SEC012N-1 NHQ CIS Client Endpoint Protection Support Service(NHQ Local) and SEC012N-2 NHQ CIS Server Endpoint Protection Support Service (NHQ Local).

Available on

- PUBLIC (U950)
- ATHENA (N950)
- MAGELLAN (R950)
- PSN (N954)
- ESS (R952)
- ESS/MWB (R955)

Service Prerequisites



- INF001N
- INF004N
- WPS001N
- PLT006N
- SEC011N
- OTH001N

Underlying Services

N/A

Standard Service Support Levels

Support Window	Availability Target	Restoration Time (P0/P1)
During Support Hours	99.9%	1 hour
Outside Support Hours	99.5%	4 hours

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

- **Service Unit:** 1 Endpoint device

SEC014N NHQ Crypto Management and Logistic Support Service

Service ID: SEC014N

Service Name: NHQ Crypto Management and Logistic Support Service

Service Type: Customer Facing / Supporting Service

Portfolio Group: Security Services

Service Status: Available

Service Background:

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description:

The NHQ Crypto Management and Logistic Support Service provides operations and management of the Cryptographic devices and keys at NHQ and authorised remotes sites following NATO policies and guidance.

Value Proposition:

Reliable management of crypto devices and keys. Enabling of policy compliance and security, and the confidentiality, integrity and availability of data at rest.

Service Ordering and Request

Service requests are initiated through the NHQ Service Request Portal on the Intranet.

Service Features:

- **Data at Rest IA Services**
 - Provision of NATO Offline Crypto Equipment (NOLCE) keying Authority.
 - Distribution and keying of all NATO Offline systems (Eclypt, SIR, Flagstone, etc.).
- **SECTRA Secure Voice Mobile Key Support**
 - Key Generation (KGC)
 - Crypto Key and SECTRA Device management
 - Assist remote sites during the keychange
 - Replacement and re-introduction devices into the network
 - Manual rekey of existing devices
- **Crypto Management and Logistic Support**
 - Cryptographic Device Procurement Support
 - Advice on the design scope and planning for the procurement of NATO-approved cryptographic solutions, and execute the procurement and potentially provide the related services: implementation, training and maintenance.
 - Operational Control of the Crypto Forward Support Points.
 - Provides Operational Control and Management of the Crypto Forward Support Points NATO-wide. Provision of timely replacement equipment and testing of faulty equipment prior to evacuation into the maintenance chain.
 - Cryptographic Keying Material Distribution
 - The timely distribution of operational keying material and equipment to the end-user.
 - Allocation of keys to service requests (SRTS).
 - Provision of Controlling Authority services for all operational (theatre) and most operational (non-theatre) physical and electronic keying material.
 - Centralised management of distributed Crypto IP equipment providing the encryption of classified data (up to CTS level).
- **Cryptographic Integration Services**
 - Installation Site Survey: Provision of Initial Site Surveys in order to deliver specialist implementation and physical security advice prior to installation of cryptographic equipment or implementation of systems with a cryptographic component.
 - Cryptographic Equipment Installation: Installation of Cryptographic Devices at NATO HQ authorised locations.
 - Production of IP Data Configuration Sheets: Production of user configuration data sheets for IP encrypted links.
 - CIS System Management Support: Support to NCI Agency System Managers (and others) in the location, installation and on-site trouble shooting of systems.

Service Flavours:

The Service is available as a single flavour at the unit cost of 1.

Service Available on:

- ATHENA (N950)

Service Prerequisites:



- SEC014

Underlying Services:

N/A

Standard Service Support Levels:

Service Availability: N/A

Service Restoration: N/A

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price:

- **Service Unit:** 1

SEC015N NHQ Security Certificate Service

Service ID: SEC015N

Service Name: NHQ Security Certificate Service

Service Type: Supporting

Portfolio Group: Security Services

Service Status: Available

Service Background:

This service is owned by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description:

Provides Certificate Authority, Revocation and Lifecycle Management of digital certificates/entities for both NPKI and Commercial Certificates.

This service includes both the Agency's centralised resources SEC015 as well as the local support at NATO HQ.

The effort required to provide basic support for the Clients and software that issue the SmartCards on site is included. We are currently unable to quantify the level of effort required for advanced troubleshooting on-site. This will be monitored in 2026 and may require increases in funding for the following years.

Value Proposition:

The NHQ Security Certificate Service provides two-factor authentication (2FA) access to the NHQ CIS systems using NATO PKI digital certificates. This service enhances identity verification by requiring something the user has (a certificate) and something the user knows or possesses.

By integrating certificate-based authentication with 2FA, the service significantly reduces the risk of unauthorized access due to compromised credentials. It supports secure remote access, protects sensitive systems, and helps meet compliance requirements for strong authentication.

Service Features:

- **Certificate Authority Services:**
A service used for the creation and issuance of digital certificates to end-user (both human and non-human). This service will be provided from a Registration Authority (RA). The RA will be only interface to the NATO PKI system to create and issue digital certificates. The service provided also includes the revocation process.
- **Revocation services:**
The Certificate Revocation List (CRL) enumerates the revoked certificates. This list will be checked, every time an end user uses digital certificates to establish a secure connection, or to authenticate to a system the CRL is checked. As soon as a certificate is on the CRL the connection, authentication is denied.
- **Lifecycle Management of Digital Certificates / Entities:**
Lifecycle Management of Digital Certificates / Entities is a service which contains the creation, issuance, management, maintenance, re-issuance, key recovery, revocation and deletion of a bonafide end-user (both human and non-human). The lifecycle management of digital certificates / entities also includes the partial management, maintenance of the meta directory on which the user are created.

Service Ordering and Request

The new NPKI Certificates are not ordered directly but are triggered by requesting accounts on the Networks where the Service is available.

Commercial Certificates are ordered through ITSM.

Service Flavours:

The Service is available as a single flavour at the unit cost of 1.

Service Available on:

- Commercial Certificates
 - o PUBLIC (U950)
- NPKI Certificates
 - o MAGELLAN (R950)
 - o ESS (R952)
 - o ESS/MWB (R955)

Service Prerequisites:

- WPS002N



- PLT006N
- OTH001N
- SEC011N

Underlying Services:

- SEC015

Standard Service Support Levels:

Support Window	Availability Target	Restoration Time (P0/P1)
During Support Hours	99.9%	1 hour
Outside Support Hours	99.5%	4 hours

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

- **Service Unit: 1**

LOG001N NHQ CIS Asset & Materiel Management

Service ID: LOG001N

Service Name: NHQ CIS Asset & Materiel Management

Service Type: Customer Facing / Support

Portfolio Group: Logistic Services

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The NHQ CIS Asset and Materiel Management includes CIS equipment inventory management, receipt, dispatch, storage, stock management, warehousing, internal controls, handover takeover, support equipment write-on/write-off, disposal coordination and logistic support for CIS items at remote NHQ locations. CSU Brussels performs as the single point of entry for the majority of new CIS equipment procured through common funding of NATO HQ.

Value Proposition

The Service provides multiple values:

- Serving as the NHQ hub for the majority of CIS Asset and Materiel Management activities;

- NATO common funded CIS Equipment is managed and safeguarded throughout the full materiel lifecycle process;
- Improvement of the CIS Materiel Management and availability of stock managed items;
- The centralization of storage, warehousing, receipt, dispatch, transportation, and materiel coordination functions provides cost savings to the customers at NHQ;

Service Features

- **Planning:**
Planning, scheduling, coordination and documentation update for Storage Management and Warehousing Services. Planning, scheduling and coordination for Receipt and Dispatch Services.
- **Receipt/Dispatch:**
The Receipt and Dispatch (R/D) activities are an essential element, which supports project execution, service delivery, supply management and asset management associated with CIS. This is an Asset Management activity providing identification, serialization and traceability of CIS equipment.
- **Storage:**
NHQ CIS assets are stored and managed in the CSU Brussels Warehouse as part of the Inventory Project supporting the procurement, supply, exchange, repair and upgrade processes for CIS equipment within NHQ. The Service relates to the CIS requisitioning and supply activities of the NATO HQ.
- **Inventory Management:**
The indirect or direct support is provided to the Custodian Account holder in the completion of the annual inventory activities. The support activities are related to handling of discrepancies within an account balance list. This can be associated with the annual counting process or for an individual or multiple item loss/damage report.
- **End of Life asset management:**
When an asset reaches its end of life (obsolescence, failure or loss), following actions are performed:
 - A Report Of Survey (ROS) is created
 - Physical decommissioning and disposal
 - Financial write-off
- **Asset Transfers**
The HO/TO is an essential element of inventory checking when equipment is moved from the responsibility of CSU Brussels to a Customer Custodian Account or back. The HO/TO process is required to ensure that common funded equipment is handled in accordance with the Financial Regulations and Asset Management Directives and Procedures.

Service Ordering and Request

All of the mechanisms for requesting this service are integrated into other services. There are no direct ways to request the service.

Service Flavours

The Service is available as a single flavour with a unit cost of 1.

**Available on**

N/A

Service Prerequisites

N/A

Underlying Services

N/A

Standard Service Support Levels

The Service complies with the AD 06.00.15 (Accounting for NCI Agency Assets)

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

- **Service Unit: 1**

OTH001N NHQ Service Management and Control

Service ID: OTH001N

Service Name: NHQ Service Management and Control

Service Type: Supporting Service

Portfolio Group: Other

Service Status: Available

Service Background

This service is owned and delivered by CSU Brussels and is specifically tailored to meet the unique needs of its customers. At NATO HQ, there are distinct CIS environments, unique business requirements from the International Staff supporting the North Atlantic Council (NAC) and the International Military Staff (IMS) supporting the Military Committee, as well as the NATO member nation delegations. Additionally, there are site-specific security requirements mandated by the NATO Office of Security (NOS).

Due to these requirements, the service is funded to maintain a direct and specific link with the customers, which cannot be supported financially as a standardized central service. The service is structured to align with the corresponding service in the Customer Service Catalogue, ensuring consistency, compliance, and seamless integration with existing frameworks.

The Director of ICTM has created a roadmap for migrating NHQ to Central Services over several years, depending on the maturity and availability of those services for NHQ customers. This service includes resources to maintain IT operations for back-end infrastructure, similar to a Business Area, as well as support for day-to-day operations, similar to other CSUs.

As part of CSU Brussels' Asset Replacement Plan (ARP), the investment cost for lifecycle replacement is out of scope for this service. However, the effort required for implementation falls within its responsibility.

Service Description

The Service Management and Control (SMC) at NHQ is providing and continuously improving critical IT service management capabilities and proactive system monitoring for all NHQ users, and support staff capabilities for CSU, NOS, SITCEN, IMS and ICTM. Our services ensure efficient IT operations, improved service delivery, and enhanced visibility into the health and performance of key IT systems.

In addition, enablement of the intake and management of new business requirements originating from NHQ stakeholders. Ensures alignment between operational needs and long-term portfolio planning through structured demand management, feasibility analysis, and integration into the Service Portfolio lifecycle. All major change requests and NHQ strategic capability improvements are captured and evaluated in collaboration with ICTM & IMS and Portfolio Governance bodies.

Value Proposition

This service delivers significant business value through:

- **Enhancing User Experience across all NHQ Services:**
Through a comprehensive customer portal providing access to over 250 self-service IT offerings, streamlining request submission and resolution.
- **Efficient Service Delivery:**
Automated ticket routing and defined approval workflows within the Service Management system ensure timely and accurate handling of IT requests and incidents.
- **Integrated ITSM Toolset tailored for NHQ:**
The tools required to empower the ITIL processes customized to NHQ.
- **Improved Decision Making:**
Robust reporting capabilities, leveraging data from Service Management and the Configuration Management Database (CMDB), management informed decision-making for QSLR and Change Advisory Board (CAB) processes.
- **Proactive Issue Resolution:**
Real-Time system monitoring tools enables proactive identification and resolution of potential issues, minimizing downtime and service disruptions.
- **Comprehensive IT Asset Management:**
Accurate and up-to-date information within the Discovery and CMDB facilitates effective management of IT assets (hardware and software).
- **Strategic Alignment with Business Needs:**
Facilitating the intake, qualification, and refinement of Business Requirements (BRs) and ensures these are analyzed and tracked in a structured manner. Approved BRs are reviewed for technical and architectural feasibility, prioritized based on business value and feasibility, and integrated into service improvement planning and the NHQ Portfolio list.

Service Features

This service is enabled by the following key technical components, which provide specific service features:

- **Central ITSM ticketing system - BMC Helix ITSM (a.k.a. Remedy):**
The central platform for managing Incidents, Requests, Changes, Problems, Service Assets, and the Service Catalogue, providing process automation and workflow management.
- **Configuration Mgmt. and Asset Discovery - BMC Discovery and CMDB:**
Automatically discovers and maintains a comprehensive inventory of IT infrastructure (servers, hardware, software), providing a foundation for informed decision-making and change management.

- **Reporting - BMC Smart Reporting:**
Generates insightful reports and dashboards on key service management metrics, supporting performance analysis and continuous improvement.
- **System Monitoring – Zabbix:**
Provides real-time monitoring of critical IT systems and infrastructure, enabling proactive alerting and issue identification (with basic and advanced monitoring and alerting levels).
- **ITAM - BMC Asset Management:**
Manages the lifecycle of IT assets (hardware and software), ensuring accurate tracking, accountability and usage. This provide the customer with the information needed for them to complete their responsibilities with property accounting.
- **Knowledge Base:**
A repository of information and solutions to common issues, empowering users and accelerating issue resolution.
- **Self-Service Portal (BMC DWP):**
A modern user-friendly interface for accessing the Service Catalogue, submitting requests, tracking tickets, and accessing the Knowledge Base. Provides a clear and accessible catalog of available IT services (over 250 offerings) for end-users.
- **Integrations (with iDAMS, AD, MDM):**
Seamless integration with iDAMS and Active Directory (AD) enhances data accuracy and streamlines user management within the Service Management system.
- **Request Fulfillment Management:**
Handling user requests for information, access, and standard changes.
- **Change Management:**
Controlling and managing changes to the IT environment to minimize risk.
- **IT Infrastructure Event Management:**
Monitoring system events to detect and respond to potential issues.
- **NHQ Business Intake and Requirement Tracking:**
Supporting structured intake of new service demands, features, and enhancements. Business Requirements are reviewed by the PMO and stakeholders for completeness, feasibility, and alignment with ICTM & IMS strategy.
- **NHQ Requirement Analysis and Impact Assessment:**
Submitted BRs undergo analysis involving technical leads and security experts. Outcomes feed into various Portfolio Boards and release planning discussions.
- **Portfolio Life-cycle Management:**
Supporting the full lifecycle of service portfolio items — from initial business intake and evaluation to retirement or transformation. It ensures traceability of business needs throughout their evolution into operational services. By integrating with ICTM, IMS and governance bodies, the service contributes to prioritization, alignment with strategic goals, resource planning, and service decommissioning when required. Portfolio decisions are informed by data from Service Management, BR tracking, and performance reporting, enabling continuous portfolio optimization.

Service Ordering and Request

Service requests are initiated through the NHQ Service Request Portal on the Intranet. Incident and support requests follow standard support workflows.

Service Flavours

The Service is available as a single flavour with a Unit cost of 1.

Available on

The Core Software is only installed on Magellan and Athena with additional software components deployed on other NHQ networks.

Network	ITSM	ITAM	Reporting	Monitoring
Public (U950)		X		X
Athena (N950)	X	X	X	X
Magellan (R950)	X	X	X	X
PSN (N954)		X		X
ESS (R952)		X		X
ESS (R955)		X		X

Service Prerequisites

- INF001N
- INF004N
- PLT006N
- SEC011N

Underlying Services

N/A

Standard Service Support Levels

- **Service Availability & Service Restoration:**

Availability Target	Restoration Time (P1)
99 %	1 Day

Service Reporting

Reporting is provided during Quarterly Service Level Review (QSLR) meetings.

Available NCI Academy Training not covered by service cost:

N/A

Service Cost / Price

- **Service Unit:** 1

Appendix 1 – Underlying Services

INF046 Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service

Service ID: INF046

Service Name: Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service

Portfolio Group: Infrastructure Services

Service Description: NATO Registration Service comprises data collection, metadata tagging, data quality curation, master data management (MDM) and reporting.

NRA SME work with clients to create Alliance-wide unique master data records within NATO's Technical Registry, protecting against duplicates, ambiguity and sprawl using idempotent transactions and continuous quality inspection. In addition to managing the master data through various change lifecycles, NRA offers CIS situational awareness services to subscribers.

Through matching, consolidation, and the application of standard formats and structures, data is leveraged as both technical and business information, to be made available for analytics and decision support.

Value proposition: NRA services provides value to customers through the collation and sharing of centrally registered items Alliance-wide, improving data integration, assuring global uniqueness, and protection from collisions in names, numbers and semantics. As organizations become data-enabled, simultaneous with an accelerating data velocity, the criticality of master data management has grown to be an imperative.

Service Features: • IPAM (IP Address Management) – This service is responsible for maintaining a global network address registry enabling assignment of unique numbers. These networks receive identity attributes drawn from the registration of hosts, customers, DNS resource records and graph labels. All records are monitored for utilization and managed through changes.

Service Flavours: NRA offers different flavours according to different data spheres

INF046-DDI: Fulfils the IPAM requirement to register and manage IPv4 address allocation and assignments. This entails maintaining the accuracy of NATO's records for use on the FMN & AFS networks. In support to NATO entities and missions the NRA manages address allocation. The NRA is also responsible for maintaining Network information in IRR (Internet Routing Registries), this information is used by ISPs for managing NATO's Internet traffic.

As NATO POC to the Internet community, NRA also approves and registers all renewed FQDN (Fully Qualified Domain Names) provided by NATO for use by any NATO website, even beyond NCIA administrative borders.

Further registrations such as IS-IS and URN/OiD fall under this flavour.

INF046-B WHOIS Lookup: a "white pages" service to lookup network endpoint identity attributes. The goal is to provide situational awareness of ICT infrastructure for the Alliance, that is:

- o Mission critical (e.g. Cyber and Network Operating Centres)
- o Up to date
- o Accurate
- o Unambiguous
- o Consumable

This service is offered in both Web and API interfaces.

Available on:

All Networks

Service Prerequisites: NATO member, NS nation connection is behind a NNG (AFS) or for a none-NATO nation, the MS connection is behind a NIP (FMN)]

Standard Service Support Levels:

Service Availability¹ Target: *[During heavy load times BAU requests will receive lower priority than mission critical warfighting requests. Registration and allocation services work on a 2 week (10 working day) delivery window, however this may be further delayed if provided information is not thorough and correct. This delivery window is to facilitate clarifications, ensuring forward planning and data integrity; once registration and allocation are complete, a new ticket must be raised for changes and amendments not in the original ticket.]*

Service Restoration: *[For service degradation NRA will act (MTTR) within 1 working day of an incident notification, NB in some instances full restoration will be beholden to the vendor timelines and availability.]*

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.]

Service Cost / Price: [This service is costed to cover the Sponsorship fee (ECIS), administration and overheads by the NRA (Calculated in TAS hours SSC).

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes

INF046-A costed per IPv4 address. Each address is costed at 0.19. For none registration related work this is costed in TAS hours towards a project a full breakdown of costing is provided on the NRA Wiki.

INF046-B costed per subscription. An annual subscription enables access to query the database via the webUI (askNRA) or the whois-RFC protocol. A subscription costs ~20 TAS (€2500) per team and may be shared over multiple accounts, however account credentials may not be shared between individuals. The API key is charged at 40 TAS (€5000) per APIkey, an APIKey is tied to an endpoint and may not be reused.

INF051 Enterprise Edge Service

Service ID: INF051

Service Name: Enterprise Edge Service

Portfolio Group: Infrastructure Service

Service Status: Available

Service Description: Enterprise Edge Service comprises the set of services, which support secure communications across network boundaries and support services within specific boundaries. The Enterprise Edge Service enables the secure communication between NR domains, NU domains, NATO Cloud Environments and the Internet.

Value Proposition: Enterprise Edge Service enables the capability for services to communicate securely across network boundaries through secure edge services.

Service Features:

- Dynamic Host Configuration Protocol (DHCP) –Enterprise / Mobility / Guest Wifi
- Domain Name System (DNS) – External lookups from Internal clients and services
- Network Time Protocol (NTP) – Internet NTP feed for services
- Network Load Balancer with Web Application Firewall – Connectivity between domains Internet / NR, Internet / NU, Cloud / NU, NR / NR, NR / NU
- Secure ICAP Gateway with Data Loss Prevention
- Simple Mail Transfer Protocol (SMTP) Gateway
- Remote Desktop Gateway – NR / NU
- Secure Client Remote Access
- NATO Public cloud (NPCL) remote acces and email services.

Service Flavours: The service is available in the following flavours:

- **INF051-A Infrastructure services**
These services are underlying services for most of the agency services. They consist of the following sub-services.
 - **INF051-A-1 Centralized NTP, DHCP, DNS services**
This service provides fundamental DHCP, DNS, NTP services to the agency as a whole.
 - **INF051-A-2 Secure Load Balancer with Web Application Firewall**
The secure load balancer capability serves as intermediate connection between services or clients and a web application server. The Web Application Firewall provides an added layer of protection by protecting the backend server from direct connection, intercepting traffic to inspect and block malicious content, provide web application firewall (WAF) functionality, and perform load balancer functions between multiple backend servers. Data Loss Prevention can be added to this service in order to prevent the upload of classified material.

- **INF051-A-3 Remote Desktop Gateway**
The Remote Desktop Gateway capability provides a secure encrypted connection to a remote host via RDP. It provides granular control over remote connections by forcing policy based access control on the individual sessions. This service is traditionally used to administer servers on a lower classification network from a higher classification network (NR access to administer NU Servers).
- **INF051-B e-mail services.**
This service flavour is underlying to the on-prem NDWC email services. It manages the SMTP gateways. SMTP Gateways ensure secure email communications between disparate networks. The SMTP Gateway includes email routing, antimalware, antispam, data loss prevention and email address rewriting. These gateways are essential to ensure the security of both inbound messages and outbound messages.
- **INF051-C NATO Public Cloud (NPCL) e-mail services.**
This cloud-based service is a similar service as the INF051-B email service. It manages the cloud SAAS SMTP infrastructure on the NATO Public cloud infrastructure, securing the inbound and outbound messages on Microsoft 365.
- **INF51-D NU Remote Access VPN.**
Remote Access VPN provides the on-prem Virtual Private Network infrastructure required for remote access from Enterprise Managed Mobile Devices to Enterprise Networks. This consists of the VPN Concentrators which secure remote access connections for PAN Mobility (NU PAN). The capability includes the use of Multi-Factor authentication, Network Access Control, Client Posture Assessment and Client Remediation.
- **INF51-E NR Remote Access VPN.**
Remote Access VPN provides the on-prem Virtual Private Network infrastructure required for remote access from Enterprise Managed Mobile Devices to Enterprise Networks. This consists of the VPN Concentrators which secure remote access connections and Reach (NR AIS). The capability includes the use of Multi-Factor authentication, Network Access Control, Client Posture Assessment and Client Remediation.
- **INF051-F NATO Public Cloud (NPCL) remote access services.**
This cloud-based service is a similar service as the INF051-C Remote acces VPN service. It manages the cloud Secure Access Services Edge (SASE) infrastructure on the NATO Public cloud infrastructure. This infrastructure is providing Zero Trust Network Access (ZTNA) to the users of the service.
- **INF051-G Scientific Wi-Fi services.**
This cloud-based Secure Web Forward Proxy service is providing secure means to browse Internet from the Scientific Wi-Fi through Zero Trust Network Access principles.



It provides customizable filtering methods to access the networks by category or explicit white list. The service includes SSL Interception, antimalware protection.

Available on:

NATO Unclassified

NATO Restricted

NATO Cloud Environments

Service Prerequisites:

INF003 Enterprise Internet Access (For DMZ services to the Internet / Cloud)

INF004 Infrastructure Hosting Service

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Ops Centre personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Contact Centralized service desk: 626 3177 (NCN) or the commercial number
Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Cost / Price: As an underlying service, its cost is distributed across other customer facing services rates.

INF063 Enterprise DataCenter LAN Service

Service ID: INF063

Service Name: Enterprise DataCenter LAN Service

Service Type: Customer facing Service

Portfolio Group: Infrastructure Services

Service Description: DataCenter is a service that will enable users to access centralized services and application and supports Infrastructure as a Service (IaaS) / Platform as a Service (PaaS) services within NISC (storage, Hosting, Infrastructure backup and Archive). The Enterprise DataCenter LAN service is crucial to enable collaboration and communication for applications and services.

Value Proposition:

DataCenter Services aims to facilitate the customers to use the centralized services and applications hosted in the DataCenter and processing of applications and data by providing high capacity, high density and high features switching capabilities combined with high-speed links for the intra-DCcommunication.

Available on:

- NATO Unclassified
- NATO Restricted
- NATO Secret
- Mission Secret (when invoked)

Service Prerequisites:

RLS001 Real Life Support
 INF014 Transmission Service
 INF002 NGCS PoP Service
 SEC011 Gateway Security Service
 SEC014 Crypto Management and Logistic Support Service
 INF005 Infrastructure Integration Service

Standard Service Support Levels:

	Availability Target	Service Response*				
		P1	P2+	P2-	P3	P4
INF063	99.5%	1 hour	2 hours	2 working hours	8 working hours	16 working hours

* Working hours in Central European Time zone (CET).

* ESOC available 24/7, for P1 and P2+ Incidents out of working hours, on-call L2 Support Staff available within 1 hour (P1) / 2 hours (P2+), to remote support Incident resolution.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) Restoration Time is 4 (four) hours with 80% INC IN SLA Enterprise-wide. Spare hardware is required in order to meet the above restoration times.

N.B. Service will be restored under the condition that underlying services are available. Priority Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per TOR (Top Of Rack) switch. For 2026, the services is available only in Enterprise Datacentre locations notably: Shape (DW2), Lago Patria (DW3) and The Hague (DW5). Please see Service Rates document for standard rates applicable to the service.

SEC008 Cyber Security OPCEN Helpdesk Service

Service ID: SEC008

Service Name: Cyber Security OPCEN Helpdesk Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: Cyber Security OPCEN Helpdesk Service provides the customers with a single point of contact for cyber security related incidents, requests and advice, as well as for cryptographic equipment configuration and keying. This service is a 24/7 provided service.

This service provides assurance that:

- cyber security incidents are reported to a single point of contact and correctly escalated;
- customers have a single point of contact to push requests or ask for advice from any NCSC organizational entity;
- crypto-related issues are reported to a single point of contact;
- customers experiencing crypto configuration issues are helped in applying the configuration changes needed to operate properly TCE crypto devices;
- NPKI certificate related requests (issue, revoke) are raised to a single point of contact.

Value Proposition: Support to Cyber Security – Defence. Continually accessible advice and action to support the customer in the maintenance of efficient and compliant cyber security and cryptography that underpins the security of our communication and information.

Service Features: This service is comprised of the following features:

1. **SEC008/1: 24/7 single point of contact for cyber security related incidents, requests and advice:** 24/7 presence of specialists to give advice on potential cyber security incidents (and appropriate escalations as required) and 24/7 helpdesk for reporting the cyber security incidents (SEC006) and the ITIL incidents related to NCSC services. Cyber Security Incident management Service provides COMSEC and COMPUSEC, incident violation and insecurity investigation. The service enables an effective and efficient response to immediately contain a detected and/or reported incidents, including incident containment, eradication, recovery and follow-up.
2. **SEC008/2: 24/7 helpdesk for IP Crypto devices:** Operation of IP Crypto Central Management System and 24/7 helpdesk to support cryptographic equipment issues, CRYPTO key changes coordination, verification and reporting, troubleshooting and ITIL Level 1 and 2 support.
3. **SEC008/3: 24/7 support for cryptographic devices installations:** 24/7 support to new cryptographic devices installations or changes to existing infrastructure, including Production of user configuration data sheets and Creation of units into the IP Crypto Central Management System.

4. SEC008/4: **Creation and revocation of NATO PKI certificates:** Provides a 24/7 single point of contact for creation and revocation of NATO PKI certificates.

Service Flavours: The Service is available as a single flavour.

Service Available on:

All NATO networks for SEC008
NSV2 for SEC008
NNCCRS for SEC008
SIGINT COINS for SEC008
NRF MS for SEC008
NRF NS for SEC008

Service Prerequisites:

This service has the following dependencies

SEC006 - Incident Response
SEC014 - Crypto Management
SEC015 - Security Certificate (NPKI)

Underlying Services: OTH001, TRA002

Standard Service Support Levels: 24/7

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC020 Cyber Security Management Service

Service ID: SEC020

Service Name: Cyber Security Operations Management Service

Service Type: Supporting Service

Portfolio Group: Security Services

Service Description: Cyber Security Operations Management Service underpin and enable the delivery of the other NATO Cyber Security Centre (NCSC) Services.

Value proposition: Cyber Security Operations Management Service facilitate the effective, efficient and resilient delivery of all other NCSC services. The service provides the essential capabilities that underline the provision of NCSC's portfolio of Cyber Security Services, in particular the people, resource, materiel and management essential to their operational delivery.

Service Features:

Acquisition Support: Acquisition support activities to procure the necessary external CIS required for the delivery of NCSC's cyber security services in compliance to NATO Financial Regulations for transparency and competitiveness. This may include the procurement of annual hardware support and software licenses, professional support services, outsourced support contracts, and consumables and sundry items.

Business Management Support: Planning and execution of NCSC business, financial, resource, logistics, training coordination, operational deployment planning, travel, and personnel related activities. Review, creation, maintenance, distribution, and advising on NCSC business, financial, resource and personnel planning project plans and documents. Coordination of NCSC logistic requirements, development and management of the NCSC budget, leading the submission of Medium-Term Financial Plan (MTFP) bids and management of all procurement requirements. Includes NCSC level travel coordination and liaison.

Service Delivery Management Support: Acting as a source of expertise and single point of entry for NCSC Service Level Management activities, including: service catalogue and Service Level Agreement (SLA) reviews, formation of metrics and KPIs, monthly and quarterly reporting, contingency planning, change management, and configuration management. Liaison with internal and external customers to ensure mutual agreement on the evolution of NCSC's services.

Project Management Support: Management of projects according to PRINCE2 methodology. This service includes the definition of acquisition requirements and contracting strategy, followed by a competitive outsourcing to industry from the 30 NATO nations. It includes as well partnering with industry to ensure that the latest, state-of-the-art technology is implemented in a coherent and cost-effective way.

Architecture Support: Architecture expertise to ensure the evolution of NCSC services are coherent with the overarching direction of NATO's technical CIS architecture.

Assessment of customer requests and solution approach to recommend the set of NCSC services necessary to be compliant to NATO security directives.

Internal IKM and Administrative Support: Cyber Security Information Knowledge Management: Management of the content of all the data-centric CIS Security systems, ensuring the coherence and the accuracy of all the data stores used by CIS Security Capabilities. Day-to-day administrative support to ensure smooth operation within the NATO Cyber Security Centre.

Service Request: Inherent to delivery of other NCSC Cyber Security Services.

Service Flavours: Service is available as a single flavour.

Available on: Network neutral

Service Prerequisites: None

Underlying Services: OTH001, TRA002

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC101 – NCSC Coherence and Service Management

Service ID: SEC101

Service Name: NCSC Coherence and Service Management

Service Type: Underlying

Portfolio Group: Security Services

Service Description: The NCSC Coherence and Service Management (SEC101) service provides the governance, processes, and resources required to deliver secure, reliable, and continuously improving IT capabilities across the NATO Cyber Security Centre (NCSC) landscape. Acting as a shared underpinning function, the service maintains the master service catalogue, orchestrates changes from concept through deployment, manages supplier engagements, and drives continual service improvement. By integrating service management best practices with robust security oversight, SEC101 safeguards service integrity while enabling agility and innovation.

Value Proposition:

Catalogue Management – A consolidated service catalogue and artifact repository eliminate duplication and confusion, giving stakeholders clear visibility of available services and their status.

Change management & transition assurance – Structured CAB governance, configuration management, and release practices reduce the risk of outages and accelerate time-to-value for new capabilities.

Data-driven performance – Regular SLT/KPI/KQI reporting enables proactive management, helps prioritise improvements, and demonstrates measurable value to the business.

Vendor management & cost optimisation – Centralised contract oversight, rate-card management, and SmartSourcing initiatives ensure spend is controlled while capacity scales to meet demand.

Continuous improvement culture – Obsolescence management and CSI initiatives keep the environment secure, compliant, and future-ready without disruptive, large-scale projects.

Service Features:

Service Management Support function ensures the effective delivery and continuous alignment of services with business goals. It encompasses the management of the NCSC service catalogue and associated artifacts, enabling clarity and consistency across service offerings. This area also oversees service change activities, including the facilitation of SLA Change Advisory Boards (CABs) and the calculation of service rates to ensure financial and operational viability. A core component is the administration of service agreements—such as SLAs, SSPs, OLAs, and POWs—which define expectations and responsibilities across stakeholders. Performance is closely monitored through the consolidation and reporting of service-level metrics, including SLTs, KPIs, and KQIs, on a monthly and quarterly basis. Additionally, this area supports dynamic customer and stakeholder engagement, responding

to ad-hoc inquiries from ACO, OCIO, and CYOC. It also manages various service-related taskers, ensuring that operational priorities are met with agility and responsiveness.

Service Transition Support function ensures smooth, controlled implementation of changes across the NCSC environment, minimizing disruption and ensuring service readiness. It leads the coordination of the NCSC domain CAB, managing all types of change—from internal operational updates and CSI initiatives to the integration of project deliverables. This includes overseeing the full change management process to ensure structured assessment, approval, and alignment with business priorities. The team supports the transition of improvements into live operations, whether driven by efficiency goals or project outcomes. Configuration management ensures accurate system records for impact assessment, while release and deployment management provides consistent, well-planned rollouts with proper testing, communication, and stakeholder engagement.

Service Resourcing and Contracting function ensures effective vendor engagement, procurement oversight, and resource alignment to support both ongoing service delivery and strategic evolution. It maintains a current supplier register and manages relationships with vendors and account managers, while also overseeing the external contracts repository for accuracy and accessibility. The team supports the timely submission of mandatory documentation, including MYCA and DR, and ensures full compliance with procurement rules and regulations throughout all stages of the acquisition process. It initiates and follows up on contract renewals through the ACQ procurement plan and acts as the central point of contact for procurement inquiries, reinforced by updated “how-to” wiki resources. Procurement activities are actively monitored via ACQ and ECAM workflows, with supplier performance evaluated against defined internal KPIs. Delivery tracking is conducted to ensure alignment with timelines and service expectations. Additionally, the function supports SmartSourcing by identifying opportunities—such as CSSF and SC—that can enhance service capacity and enable scalable, future-ready operations.

Continual Service Improvement (CSI) function drives ongoing enhancement of services through a structured, data-informed approach. It identifies performance gaps, service inefficiencies, and evolving business needs by analysing operational data, stakeholder feedback, and service metrics. A critical aspect of CSI is obsolescence management, which involves proactively identifying aging or unsupported components and initiating minor replacement projects to maintain operational stability. These like-for-like replacements ensure service continuity while avoiding unnecessary complexity or cost escalation. CSI initiatives—whether efficiency improvements, compliance updates, or risk mitigations—are transitioned into live operations in coordination with change and release management to ensure sustainable and measurable outcomes. The function embeds best practices, promotes cross-functional collaboration, and ensures lessons learned are leveraged across the organisation. By aligning service performance with strategic objectives and maintaining a continuous improvement loop, CSI helps keep services responsive, reliable, and future-ready.



Service Flavours: This Service is available as a single flavour.

Service Available on: N/A

Service Prerequisites: None.

Standard Service Support Levels: P4 – 2 Business Days

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC102 – Centralised NCSC Level 1 Support (Remote)

Service ID: SEC102

Service Name: NCSC Level 1 Support (Remote)

Service Type: Underlying

Portfolio Group: Security Services

Service Description: The NCSC Level 1 Support (SEC102) service provides centralised, around-the-clock first-line support for all NATO Cyber Security Centre (NCSC) services. It acts as the primary entry point for incident reporting, service request fulfilment, and coordination of escalations to higher support tiers. Tickets are received through multiple channels—including phone, ITSM, and email—and triaged by experienced analysts who resolve known issues or initiate structured escalation to Level 2 or Level 3 teams. The centralised remote support model enhances consistency, accelerates response times, and ensures uninterrupted operational support.

Value Proposition:

24/7 guaranteed responsiveness – Two seats to provide round-the-clock coverage with a 15-minute initial response SLA.

Centralised ticket triage – A unified intake and triage model eliminates fragmentation and streamlines incident resolution and request fulfilment.

Structured escalation – Clear pathways to Level 2 and Level 3 teams ensure timely resolution of complex or critical issues.

Optimised resource usage – Underlying cost model allows services to benefit proportionally from support without separate procurement.

Enhanced operational assurance – Proactive known error management and on-call staff coordination sustain service reliability and user satisfaction.

Service Features:

Level 1 Support Operations - This function provides initial support intake via phone, ITSM, and email. Analysts handle ticket classification, impact assessment, initial troubleshooting, and known error resolution. When issues exceed Level 1 scope, staff initiate documented escalation processes and coordinate with on-call Level 2/3 support engineers to ensure timely follow-through.

Request Fulfilment and Incident Response - The service includes processing of user requests and resolution of incidents related to common access, system issues, and user-facing errors. A knowledge base of frequently resolved incidents underpins swift action and reduces escalation rates.

Escalation and Coordination - Support analysts maintain contact with on-call resources and engineering teams, providing relevant artifacts and context for escalated issues. This



structured coordination supports minimal downtime and efficient handover across time zones.

Monitoring and Metrics - Support operations are governed by performance metrics including SLA response time (15 minutes for all P0 incidents), escalation frequency, and resolution times. Monthly reports help identify training needs and improvement opportunities.

Service Flavours: Single Flavour

Service Available on: NS/NR/NU

Service Prerequisites: N/A

Standard Service Support Levels: P0 - 24 x 7

Service Cost / Price: Not possible to order separately. Service costs are underlying for NCSC services based on estimate workload weight totalling to a 100% cost distribution across NCSC service catalogue.

SEC104 – Level 1 Support to NCSC Services (On-site)

Service ID: SEC104

Service Name: NCSC Level 1 Support (on-site)

Service Type: Underlying

Portfolio Group: Security Services

Service Description:

Centralised Shared Level 1 hands-on Support through NCIA DCSUs for all NCSC Services. Underlying service to enable Centralised 1st level support where local staff presence is necessary, i.e. touch labor or site access support. Reduces the need for L2, L3 engineers to travel when there is a need for small changes (HW obsolescence replacements / upgrades / firmware updates) and incidents that are related to hardware failure.

Value Proposition:

Local touch labor – Provides essential on-site support for hardware-related incidents and system access needs.

Support for visits – Facilitates site access and logistics for 3rd parties and accreditation activities.

Engineer time savings – Reduces L2/L3 travel for routine tasks like firmware upgrades or device swaps.

Service Features:

IMACD Support – Install, Move, Add, Change, Dispose for deployed hardware.

Site Access Coordination – Escorting and support for audits, 3rd parties, and outsourcing tasks.

Local Systems Admin Support – admin level access for locally (CSU) managed systems,

Secure Storage & RMA – Local spare parts handling and returns coordination.

Obsolescence & Firmware Operations – Physical execution of replacements, upgrades, and firmware updates for ageing or failed hardware.

Service Flavours: Single Flavour

Service Available on: NS/NR/NU

Service Prerequisites: N/A

Standard Service Support Levels: P4 – 2 Business Days

Service Cost / Price: 2025 is the first year that LEG005 services were cross referenced and transferred into centralised Cyber Security services. The cost is “as is” is based on SSC and

transferred from LEG005. During year 2026 Pilot we will further breakdown activities and staff required for CSUs to meet the NCSC business objectives.

Not possible to order separately. Service costs are underlying for customer facing services based on estimate workload weight totalling to a 100% cost distribution across NCSC service catalogue.

TRA002 Education and Individual Training Delivery (EIT Delivery)

Service ID: TRA002

Service Name: Education and Individual Training Delivery

Service Type: Customer facing

Portfolio Group: Training services

Service Status: Available

Service Description: This service manages, coordinates and delivers cyberspace education and training services (EIT) to NATO, Nations, Partners and internal NCI Agency staff. The service delivers training courses and other Education and Individual Training (EIT) opportunities by the NCI Academy, an integral element of the NCI Agency. The full list of services, including a description and features, is available in the NCI Academy Cyberspace Learning Catalogue.

The service includes the provision of a comprehensive Catalogue of Cyber Learning and Curriculum along with the planning, scheduling, quality management and continuous improvement for the delivery and management of the training services listed in the catalogue and support to the students attending them.

This service includes the provision of the Academy Learning Environment (ALE) which entails the specialist IT, tools and infrastructure required to manage the service and to deliver on-site, live on-line, self-paced and blended learning.

This service does not include the NATO systems (hardware, software and applications) that are the subject of the respective courses.

This service does not include the training environment for services delivered at the customers' sites or local support from collocated Agency staff for ad-hoc, on-site training events, such as preparation of training facilities, IT training environment etc; such support must be funded separately.

Value Proposition: The training services enable the customer to use, administer and maintain other services and systems provided by the NCI Agency. This service also provides professional development training.

Service Features: The features of this service are available in the NCI Academy Cyberspace Learning Catalogue.

Service Flavours: Training opportunities are available as pre-defined in-house courses at Agency sites, through Mobile Training Teams delivered on-site at customer locations, hybrid learning, live on-line, self-paced on-line or through blended learning Tailored training will also be considered upon request.

Available on: N/A

Service Prerequisites: TRA003: Education and Individual Training Availability and Maintenance. Business prerequisites and prerequisites for individual courses as detailed in the NCI Academy Cyberspace Learning Catalogue.

Standard Service Support Levels: N/A

Service Availability¹ Target: N/A

Service Restoration: N/A

Service Cost / Price: Service prices (course prices) are provided as an annex to the NCI Academy Cyberspace Learning Catalogue. Prices for tailored NCI Academy training will be calculated upon request.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

**Minutes available during agreed reporting period excluding planned maintenance minutes*

SME005 Acquisition Service

Service description will be provided in 2027 CCSC 10.1 Version.

SME022 Maritime Broadcast Operations Service

Service ID: SME022

Service Name: Maritime Broadcast Operations Service

Service Type: Customer Facing

Portfolio Group: Subject Matter Expertise Service

Service Status: *“Available” for 2024 if approved*

Service Description: This service provides the 24/7 ability for MARCOM to manage the delivery of formal military messages onto selected HF and VLF maritime broadcasts.

Value Proposition: MARCOM is the Broadcast Control Authority for multiple High Frequency and Very Low Frequency broadcasts, used to maintain Command and Control of Nations’ vessels when placed under MARCOM C2. This service enables designated vessels to be included within specified MARCOM broadcasts, the inclusion of formal messaging traffic onto those broadcasts and the assurance of the effectiveness of the broadcasts.

Service Features: The Maritime Broadcast Operations Service includes the following broadcasts:

HF. Extends the formal messaging service onto specified NATO High Frequency (HF) broadcasts for units designated by MARCOM, as the “Broadcast Control Authority”:

1. Coordinate the inclusion of units designated by MARCOM onto the NATO X11C broadcast, including Routing Indicators and Guard List.
2. Handle traffic exceptions for traffic being directed to X11C broadcast.
3. Manage Over The Air Distribution (OTAD) for X11C broadcast.
4. Provide cover for the X11B broadcast managed by UK Commcen Plymouth, as part of and as directed by higher level NATO HF broadcast coordination.

VLF. Extends the formal messaging service onto the NATO Very Low Frequency (VLF) broadcasts for units designated by MARCOM SUBSUBNATO, as the “Submarine Operating Authority”:

1. Coordinate the inclusion of units designated by MARCOM onto the NATO VLF broadcast, including Route Changes and Guard Lists.
2. Manage the inclusion of messages when directed by MARCOM onto MARCOM broadcasts.
3. Conduct Over The Air Monitoring (OTAM) of MARCOM broadcasts to assure MARCOM that the broadcast is functional.

4. Monitoring the VLF network of VLF transmitters, receivers and others nodes, advising MARCOM of any service impacts and mitigations.

Service Request: This service is coordinated with and operationally directed by MARCOM.

Service Flavours: This service is available as a single flavour.

Available on: NS

Service Prerequisites: The service relies upon APP029 Military Messaging Application Service, INF013 VLF Broadcast Service (that provides the VLF interconnection network), CSU Northwood local service support to MARCOM for support to the 2 CMX servers (primary and backup) and 3 workstations, and upon agreements between ACO and the UK for the provision of UK HF and VLF transmitters and receivers.

Standard Service Support Levels: Any incidents impacting the service need to be submitted through the NCIA ESOC. The service consists of military personnel within CSU Northwood, plus the CMX software that is supported under annual contract with Raytheon Systems Limited, UK.

Service Availability¹ Target: 95%

Service Restoration: There are no formal service restoration targets for this service. The Raytheon support contract provides 8-hour response during normal working hours (Mon-Fri 0900-1700).

Service Cost / Price:

The service is a non-unitised service. The service cost is the approved NCIA overhead cost for the specific level of Commcen Northwood effort assigned to the operation of the maritime broadcasts, 10.75FTE military personnel, plus the annual cost of the CMX software support, enabled through UK MOD DE&S contract number GCS/00002 Amendment 1 dated 30th Janua

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP064 ITSM Toolset Application Service

Service ID: APP064

Service Name: ITSM Toolset Application Service

Service Type: Enabling

Portfolio Group: *Application Service*

Service Status: Available

Service Description: Service Management refers to the set of activities, processes, and strategies involved in planning, delivering, and maintaining high-quality services to customers or clients. It encompasses practices and frameworks used to ensure that services meet the need and expectations of Customers. Service Management often involves the coordination of people, processes, technologies, and resources to optimize the service delivery, improve efficiencies, and enhance customer satisfaction. The IT Service Management (ITSM) Toolset Application Service provides the toolset required for reaching the outcomes and benefits of Service Management. ITSM Toolset connect and automate processes underlying/enabling the management of the services provided by the NCI Agency at Enterprise and in the internal IT. The ITSM Toolset Service is an enabler of a unified platform and scalable architecture providing the foundations for managing services across their lifecycles. In particular, the Service drives the deployment of NCI Agency wide Service Management processes and service/system data collection with training and technical solutions, and provide the data warehouse for the NCI Agency Asset and Configuration Management capability and record keeping of all relevant information generated by the execution of the service management processes they support.

Value Proposition. ITSM Toolset Service enables the following functions:

- **Streamlined IT Requests:** Easily submit and manage IT support requests, ensuring timely and efficient resolution.
- **Proactive Issue Management:** Track recurring issues to identify and address the root cause, minimizing disruptions.
- **Optimized IT Operations:** Prioritize and manage IT tasks based on urgency and impact, improving overall service delivery.
- **Consistent Service Experience:** Standardized processes ensure reliable and consistent IT support for all users.
- **Data-Driven Insights:** Access valuable metrics on IT performance to inform strategic decisions and improve service quality.

Service Features:

1. **Incident Management:**
 - Efficiently log, track, and resolve IT incidents to minimize service disruptions.
 - Automated prioritization of incidents based on severity and impact.
2. **Service Request Management:**
 - Streamlined submission process for IT service requests.
 - Real-time tracking and status updates for users on their requests.

3. Problem Management:

- Identification and management of underlying issues causing repeated incidents.
- Root cause analysis tools to prevent future disruptions.

4. Change Management:

- Support for planning, approving, and implementing IT changes with minimal risk.
- Comprehensive change tracking to ensure compliance and audit readiness.

5. Configuration Management:

- Centralized repository for managing and documenting IT assets and configurations.
- Visual mapping of IT assets and their relationships to help in troubleshooting.

6. Knowledge Management:

- Access to a robust knowledge base for common issues and solutions.
- Empower users and IT staff with self-service options to resolve issues quickly.

7. Reporting and Analytics:

- Detailed reports and dashboards on IT service performance.
- Customizable metrics and KPIs to monitor service efficiency and effectiveness.

8. User-Friendly Interface:

- Intuitive and easy-to-use interface for both end-users and IT staff.
- Mobile access for on-the-go service management.

9. Integration Capabilities:

- Seamless integration with other IT and business systems for unified operations.
- API support for custom integrations and automation.

ITSM Toolset Service issue:

Customers can request the ITSM Toolset Application Service or report any incidents and problems related to its use through its core function whether it would be still available, following the standard procedure as any other service:

1. Submit a Request:

- Access the ITSM Service Portal.
- Select "ITSM Toolset Application Service."
- Complete the service request form with the necessary details.

2. Report an Incident or Problem:

- If you encounter an issue with the ITSM Toolset, log into the Service Portal.
- Go to the "Report an Issue" section.
- Select "ITSM Toolset Application Service" from the list of services.
- Describe the problem and submit the incident report.

In case the system is unavailable or for any other generic request on the ITSM Toolset service the user can always contact the first line ESD support within the Enterprise Service Operation Centre (ESOC):

3. Contact Support:

Customers can also contact the IT support team directly 7 days 24 hours via phone at +32 490 58 07 31 or call Centralised Service Desk NCN:626-3177.

4. Tracking and Updates:

- After submission, you can track the status of your request or incident report through the Service Portal.
- You will receive notifications on any updates or resolutions related to your request.

All above procedures ensure that the service requests and issues are handled efficiently and effectively, providing timely support and resolution. If there are any exceptional procedures for specific cases, they will be communicated separately.

Service Flavours:

1. APP064.1 Request Management System:

This service flavour provides a comprehensive system for managing and tracking IT service requests. It ensures that all requests are captured, prioritized, and routed to the appropriate teams for resolution. The system helps in streamlining workflows, improving response times, and ensuring that all service requests are handled efficiently.

2. APP064.2 CI Discovery:

This service flavour offers automated discovery of IT assets within the organization's infrastructure. It identifies and catalogues all components, including hardware, software, and network elements, providing a complete and accurate inventory of the IT environment. This capability helps in maintaining up-to-date records of all configuration items, aiding in effective management and troubleshooting.

3. APP064.3 Central CMDB/CMS:

This service flavour provides a centralized repository for managing and storing information about IT assets and their relationships. It supports asset management, tracking, and configuration management, enabling a unified view of all IT resources. The service also facilitates better decision-making by providing insights into the interdependencies of various components within the IT ecosystem.

4. APP064.4 Monitoring, Analysis and Reporting:

This service flavour offers advanced monitoring capabilities for IT systems and applications. It includes real-time analysis and reporting on the performance, availability, and health of IT services. By proactively identifying issues, this service helps in minimizing downtime and ensuring optimal performance of the IT environment.

5. APP064.5 SMC Orchestration and Automation:

This service flavour provides tools for automating IT processes and workflows. It enables the orchestration of complex tasks across different systems and platforms, reducing manual effort and increasing efficiency. This service also ensures consistency in the execution of IT operations, leading to more reliable and predictable outcomes.

6. APP064.6 SMC Gateway:

This service flavour acts as a bridge between different systems and applications, facilitating seamless communication and data exchange. It ensures that various IT systems can work together, even if they are built on different platforms, by providing a standardized method for integrating and transmitting data across the organization.

7. APP064.7 Product Lifecycle Management:

This service flavour supports the management of the entire lifecycle of products, from design and development to deployment and retirement. It provides tools for tracking and managing product information, ensuring that all aspects of the product lifecycle are documented and controlled. This service helps in improving collaboration, reducing time-to-go-live, and ensuring compliance with regulatory requirements.

Available on: NS, NR, (soon on MS and KFOR)

Service Prerequisites:

Prerequisite NCI Agency Customer-facing Services		
Item	Name	Service ID
1	Managed Device Service	WPS001

Prerequisite NCI Agency Underlying Services		
Item	Name	Service ID
1	User Access Service	WPS002
2	Enterprise User License Service	WPS003
3	Enterprise Services Operations Centre Service	WPS008
4	Local Area Network (LAN) Service	INF001
5	Infrastructure Hosting Service	INF004
6	Infrastructure Storage Service	INF007
7	Security Certificate Service	SEC015
8	Transmission Service	INF014
9	Infrastructure Storage Service	INF007
10	Infrastructure Backup/Archive Service	INF016
11	Information Sharing and Collaboration Platform	PLT001
12	Web Hosting Service	PLT003
13	Service Oriented Architecture & Identity	PLT004

14	Database Platform Service	PLT006
15	Service Management and Control Function	OTH001

Service Assets - Software				
Item	Name	Type	License Type	Remark
1	BMC ITSM Remedy Suite	COTS	Proprietary	
2	BMC Atrium CMDB	COTS	Proprietary	
3	Apache Tomcat AS	FOSS	Apache License	
4	BMC Discovery	COTS	Proprietary	
5	CableSolve	COTS	Proprietary	
6	PatchManager	COTS	Proprietary	
7	BMC TrueSight Operations Management	COTS	Proprietary	
8	BMC TrueSight Capacity Optimization	COTS	Proprietary	
9	MS Power BI	COTS	Proprietary	
10	BMC TrueSight Orchestration	COTS	Proprietary	
11	Mule Community Edition	FOSS	Apache License	
12	Aptean (Lascom) PLM	COTS	Proprietary	
13	Oracle Database	COTS	Proprietary	
14	MS SQL Database	COTS	Proprietary	

Standard Service Support Levels:

KPI	Target	Achievement/ Scorecard indicators
Number of Incidents resolved in SLA	80%	≥80% = GREEN <80% = RED
Incident Mean Time to Intervene - MTTI	P4	MTTI ≤ 2wd = GREEN MTTI > 2wd = RED
	P3	MTTI ≤ 1wd = GREEN MTTI > 1wd = RED
	P2-	MTTI ≤ 1h during business hours = GREEN MTTI > 1h during business hours = RED MTTI ≤ 2h outside business hours = GREEN MTTI > 2h outside business hours = RED
	P2+	MTTI ≤ 1h during business hours = GREEN MTTI > 1h during business hours = RED MTTI ≤ 2h outside business hours = GREEN MTTI > 2h outside business hours = RED
	P1	MTTI ≤ 1h = GREEN MTTI > 1h = RED
	P0	MTTI ≤ 30 min wall clock = GREEN MTTI > 30 min wall clock = RED
Incident Mean Time to Restore - MTTR	P4	MTTR ≤ 3wd = GREEN MTTR > 3wd = RED
	P3	MTTR ≤ 2wd = GREEN MTTR > 2wd = RED
	P2-	MTTR ≤ 8h business hours = GREEN MTTR > 8h business hours = RED
	P2+	MTTR ≤ 8h wall clock = GREEN MTTR > 8h wall clock = RED
	P1	MTTR ≤ 4h = GREEN MTTR > 4h = RED
	P0	MTTR ≤ 1h wall clock = GREEN MTTR > 1h wall clock = RED
Number of Service Requests resolved in SLA	80%	≥80% = GREEN <80% = RED
Service Request Mean Time to Delivery - MTTD	Simple	MTTD ≤ 1wd = GREEN MTTD > 1wd = RED
	Normal	MTTD ≤ 10wd = GREEN MTTD > 10wd = RED

Service Cost / Price:

Below prices are for Operation and Maintenance and not representative of implementation costs.

Service Size	APP064.1 Request Management System	APP064.2 CI Discovery	APP064.3 Central CMDB/CMS	APP064.4 Monitoring, Analysis and Reporting	APP064.5 SMC Orchestration and Automation	APP064.6 SMC Gateway	APP064.7 Product Lifecycle Management	Price
Small-sized Commands or Operations	Max. 100 user per year	Max. 500 Managed Assets per year	Max. 500 Managed Assets per year	Max. 1.200 requests per year	Max. 1200 requests per year	Max. 1.200 requests per year	Max. 500 Managed Assets per year	CAPEX 140K (**) OPEX (up to P2+) 900K (*)
Medium-Sized Commands or Operations	Max. 500 user per year	Max. 1.500 Managed Assets per year	Max. 1.500 Managed Assets per year	Max. 6.000 requests per year	Max. 6.000 requests per year	Max. 6.000 requests per year	Max. 1.500 Managed Assets per year	CAPEX 230K (**) OPEX (up to P2+) 900K (*)
Large Static Footprint	Max. 10.000 user per year	Max. 50.000 Managed Assets per year	Max. 50.000 Managed Assets per year	Max. 600.000 requests per year	Max. 600.000 requests per year	Max. 600.000 requests per year	Max. 50.000 Managed Assets per year	CAPEX 1.4ME (**) OPEX (up to P2+) 900K (*)
All the above Separated networks	//	//	//	//	//	//	//	CAPEX 1.8ME (**) OPEX (up to P2+) 1.3 ME
SU	Users	Managed Assets	Managed Assets	Requests	Requests	Requests	Managed Assets	

(*) cost driven by Time to Intervene up to P2+ based on contextual assessment automatic established at every ticket (2 hours on call, resilient, 5FTEs, 1 G17, 4 G15)

(**) cost subjected to commercial price models changes

OTH001 - Service Management and Control, Delivery Governance, Measurement, Reporting, and Integration Enabling Function

Service ID: OTH001

Service Name: Service Management and Control, Delivery Governance, Measurement, Reporting, and ITSM Toolset Integration-Enabling Function

Service Type: Enabling

Portfolio Group: *Other Services*

Service Status: Available

Service Description: The OTH001 Service serves as a funding vehicle to deliver both centralized and locally embedded Service Management and Control functions across the NATO Enterprise. Its primary objective is to ensure that all Operational Partners benefit from unified Service Governance, Delivery Oversight, Performance Measurement, Reporting, and Integration Enablement—irrespective of their geographic location or organizational command. To this end, NCIA develops and maintains standardized ITSM tools and processes that provide consistent and equitable support to the entire customer base. OTH001 represents, in essence, a governance and control function rather than a conventional service. It operates through a combination of centralized SMC teams and SMC-supervised personnel embedded within CIS Support Units (CSUs) and Business Areas (BAs). This structure ensures that diverse operational requirements are met while preserving the benefits of central oversight and localized responsiveness.

Value Proposition. Service Management and Control, Delivery Governance, Measurement, Reporting, and ITSM Toolsets Integration-Enabling Function: OTH001 Service ensures Operational Partners that the Service Management and Control (SMC) Function, within the Chief Service Operations (CSO), holds “Service Management Authority - Operating CIS Authority” (SMA-OA) and the CIS Provisioning Authority (CISPA) within NCIA owned and managed networks. As defined in NATO Term (TTF 2022-0176), SMC provides the centralized operational mechanism enabling CSO to exercise mission-specific authority over CIS services and to adapt service delivery to evolving operational demands. SMC provides strategic oversight, governance, and policies for the full service lifecycle (implementation, control, and monitoring) across NATO enterprise IT infrastructures (incl. federation with Nations), supporting internal and external CIS Service Providers (Business Areas and Industrial Partners) with a Service Management framework through which meeting the Operational Partners’ requirements.

The SMC function provides:

- **Strategic Oversight:** Provide Service Delivery governance across the service lifecycle with a monitored strategy and roadmap (e.g. QoS Monitoring and Reporting Plan (QMRP) is one of the elements). SMC thus ensures coherent, secure, and mission-focused CIS service management across NATO Enterprise. Engage with Nations in the service management federated context.

- **Service Governance:** Align service design of new capabilities and ITSM toolsets with service management frameworks, portfolios, and catalogues; ensure coherence with acquisition strategies, policies, and procedures.
- **Governance and ITSM Toolsets Alignment and Integration:** Ensure Governance and support to SMC Enterprise Tools and processes interfaces in alignment with Agency policies and strategies; develop and maintain the SMC Reference and Target Architectures (SMC RA & TA) in cooperation with NCIA Chief Technical Office (CTO), ensuring their alignment with the Agency's current Enterprise Architecture (EA).
- **Change Management (ChM):** Define and govern the enterprise Change Management process, ensuring that change control mechanisms minimize risk and disruption.
- **CIS Lifecycle Configuration Management (LCM):** Govern the configuration lifecycle, accuracy, and traceability of all Configuration Items (CIs) across the enterprise, ensuring controlled and auditable CIS configurations.
- **Service Level Management (SLM):** Establish together with the Account Manager and monitor SLAs, ensuring agreed service quality.
- **Analysis Reporting:** Play the role of Data Owner, Producer, Steward, Analyst, and Administrator for Service Delivery at Enterprise level, coordinating the effort at Component and Element levels.
- **Risk Management:** Deliver regular (during Quarterly Service Level Review meeting - QSLR) risk reporting on service delivery.
- **CIS Provisioning Authority (CISPA):** Exercise second line responsibilities of the CIS execution and primary contact for the CIS Operational Authorities (CISOAs); Ensure that service risk is communicated.
- **Continual Service Improvement (CSI):** Define, implement, and govern CSI framework. Reports evolution of the NCIA CSI and QMRP at the QSLR. Monitor the development and execution of related Service Improvement Plan (SIP) by the concerned Business Area(s).
- **Problem management (PrM):** Define, implement, and govern PrM processes. Reports Problem Management outcomes at the QSLR.

Service Features]¹

10. IT Change Management (IT ChM) Governance

- Governs IT Change Management activities throughout NCIA.
- Assesses and supports Enterprise level changes with appropriate change categories.
- Enables and control local changes within Business Area (BA) areas of responsibilities to minimize or prevent service interruptions and to deliver services as incorporated with necessary changes and enhancements.

11. Enterprise Change Advisory Board (Ent-CAB) and Distributed Change Advisory Board (Dist-CAB)

- The Ent-CAB will manage normal and emergency changes that potentially have a major disruption and/or impact on the delivery of C4ISR service(s) to the Customers or NCIA and will manage any escalated change from the other CABs.

¹ Disclaimer: Performance of listed Change Management, Configuration Management, Release and Deployment Management, Service Level Management & Reporting and Problem Management functions are available for the accounts only if the local entities (CSUs) are funded through the respective SLAs.

CAB Membership is made up of stakeholders from the CABs and key stakeholders (incl. Customer SMEs where/when needed) who review changes and have sufficient knowledge and decision authority for their AoR.

- Other-CAB will manage normal and emergency changes that have local scope and effect.

12. CIS Life Cycle Configuration Management (LCCM) Governance and Configuration Management Boards

- Develop, own, and maintain the enterprise-wide CIS Lifecycle Configuration Management framework and the Configuration Management Data Base / System, ensuring standardization, coherence and consistency across NCIA products and services
- Through its Configuration Management System, LCCM Governance enables the consolidation of information into a single source of truth, maintains an effective and efficient LCCM Process framework and guides stakeholders through the LCCM processes. LCCM supports Asset Management, and generated all reports on CIS Configuration Management.

13. Release and Deployment Management (RDM) Governance and RD Boards

- Release and Deployment Management (RDM) aims to plan, schedule and control of releases through testing and deployment into the live environments. Its primary goal is to ensure that the integrity of the live environment is protected and that the correct components are released in line with industry good practice i.e. ITIL framework. RDM ensures testing and necessary roll back measures are in place and conducted prior to authorisation and deployment of a release or change into the live environment

14. Patch Management Governance and Patch Management Board

- The Patch Management process is essential to ensure that the correct patching steps are documented and strictly followed against the risk and/or potential threat to the NCIA's software/systems, services and managed networks. Keeping the networks secure is one of the core missions of the NCIA.
- Patch management process is performed by Business Areas and controlled by SMC.

15. Service Level Management (SLM)

- Collects and understands service level requirements, then reflects agreed commitments in Service Level Agreements (SLAs) and associated contracts for service provision.
- Contributes to SLA negotiations in terms of SLM related requirements and prepares SLAs relevant sections/annexes reflecting the service target levels that NCIA can commit to.
- Performs SLM tasks addressing approved new reporting requirements, target levels and KPIs.
- Manages NCIA KPI Dictionary and Catalogue.

16. Service Level Reporting

- Service Level Reporting enables production of the formal reports and Dashboards to the Operational Partners as committed in the providing awareness to all NCIA Service Delivery stakeholders.

- Provide all necessary raw data and analysis insights to the reporting personnel throughout the NCIA.
- Reports to prove realized levels of service (s) performance against the agreed service level targets as stated in agreements and associated contracts.
- Initiates and tracks any associated CSI, reporting, performance analysis related action items from QSLRs and SLA CABs and improvement activities.

17. Service Monitoring Governance and Business Data Analysis

- Supports and enables service level reporting with governance on data mapping, , integration of reporting tools, establishing authoritative and trusted Service Delivery data sourced to automation report and visualization functions.
- Performs data collection from monitoring tools/environments, data management (through data Extraction, Transformation, and Loading process), converting data into information and making available in user front-ends (such as reporting portals and dashboards as listed in SLAs).
- Perform Service Delivery Data Performance analysis and Data Performance trends analysis, supported by respective Business Area, in preparation of QSLR and or other reporting meetings.
- Maintains existing KPIs as well as designing and implementing new/updated KPIs as approved in SLA negotiations.
- Technical operations to maintain and continually improve the data warehouse and relevant technical operations.

18. Problem Management (PrM) and Problem Management Board

- Govern the NCIA Enterprise process and operational approach to Problem Management across all Business Areas and CIS Support Unites through means of the Problem Governance Board (PGB).
- Analyse recurring Incidents or the correlation of multiple incidents to specific services, events or locations with the aim to reduce the Mean Time to Resolution (MTTR) or prevent their occurrence altogether.
- Coordinate problem investigation and related Route Cause Analysis (RCA) with relevant Subject Matter Experts (SMEs) and trigger remediation of findings through change, risk, knowledge management or Continual Service Improvement initiatives.
- Establish Problem Management Tiger Teams for major incident assessment in order to prevent additional major incidents or future impact on provided services.

19. Continual Service Improvement (CSI)

- Govern the NCIA Enterprise process and provide guidance to all NCIA entities related to continual improvements of services, End to End service delivery or activity that results in Customers' operational or NCIA business optimization.
- Coordinate, track and manage the Enterprise CSI register in close coordination with Risk, Problem and Service Delivery Management practices.

20. Exercise and Operations support (limited to the SLA commitment)

- Develops, implements and manages in coordination with the NATO CIS Group (NCISG) all required Service Management processes and required toolset, both for static and deployable NATO CIS assets on support to the NCIA supported exercises from the Military Training and Exercises Programme (MTEP) for the NATO Command Structure (NCS), NATO Force Structure (NFS), NATO Centres

of Excellence (CoE) and the NATO nations and partners, including VeVA and ARF related exercises.

- Creates stabilisation for deployable teams, by ensuring deployment of standardised processes and procedures, which in turn increases security and interoperability.
- SMC liaises with the operational partners with respect to Service Management Governance for the management and execution of NATO CIS infrastructure and processes.
- Ensures that harmonised methods and procedures are used to provide effective control for all changes in the mission service infrastructure including service assets, configuration items and associated documentation.
- Aims to reduce the risk to the availability, performance, security and compliance of the mission services impacted by any change.
- Reduces the impact on service availability or degradation, by scheduling deployments only approved and fully tested changes of products included in operational baseline, which will aid with reducing the number of incidents raised.
- Ensuring that effective control of Configuration Items (CIs) used within the Mission network is completed. This involves identification, classification and specification of all configuration items (CIs) and the interfaces to other processes and data.

Service Flavours:

This is a standard enabling service without any flavours.

Service Prerequisites:

Prerequisite NCI Agency Customer-facing Services			
Item	Name	Service ID	Service Owner
1	ITSM Tool Application Services	APP064	Chief SMC

Prerequisite NCI Agency Underlying Services			
Item	Name	Service ID	Service Owner
1	Infrastructure Hosting Service	INF004	Chief NISC
2	Infrastructure Network Service	INF005	Chief NISC

KPIs / Reports:

Service Feature	KPI/ <u>Report</u> ^[1]	Service Level Target ^[2]
IT Change Management	Volume of Enterprise Changes assessed by NCIA Enterprise CAB and Distributed CAB ¹	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
IT Change Management	Volume of Emergency Change Requests assessed by NCIA Enterprise CAB	Minimum Frequency: monthly to Customers SME; Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Change Freeze	Volume of Change Freezes assessed by NCIA Enterprise CAB	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Lifecycle Configuration Management		Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Release & Deployment Management	Volume of Enterprise Change Requests validated by Release & Governance Board	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Patch Management	Volume of Battle Short, Emergency and normal patching requests assessed by NCIA Patch CAB	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR

^[1] This Table lists the reports (metrics), which are descriptive on the outputs of each feature. Trend analysis is available a well throughout the fiscal year in quarterly basis.

^[2] Target levels are applicable for KPIs, therefore they are marked as N/A in this table. KPI ofr reports should be the minimum frequency of the delivery of this reports

¹ When the mapping from legacy services will be completed.

Service Feature	KPI/ <u>Report</u> ^[1]	Service Level Target ^[2]
Service Level Management	Volume of SLM requirements assessed and coordinated by SLM	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Service Level Reporting	Delivery Rate of QSLR Reports to Operational Partners (% , actual/planned)	100%
Service Level Reporting	QSLR Lifecycle completion status (60 calendar days ending with review meeting and Minutes dissemination)	No delay per each account
Problem Management	Volume of Problem Records assessed by PGB	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Continual Service Improvement	Volume of CSI items managed in Enterprise CSI register	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Exercise Change Management	Volume of Changes assessed by Exercise dedicated CAB	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Exercise Change Management	Volume of Emergency Change Requests assessed by Exercise CAB	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Exercise Release & Deployment Management	Volume of Exercise Change Requests validated by Exercise Release & Deployment Manager	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
VeVA Core MN Change Management ¹	Volume of Changes assessed by VeVA Core MN dedicated CAB	Minimum Frequency: monthly to Customers SME; Summary and

¹ VeVA Core MN Change Management currently not funded within this service

Service Feature	KPI/ <u>Report</u> ^[1]	Service Level Target ^[2]
		exceptions at the QSLR
VeVA Core MN Change Management ¹	Volume of Emergency Change Requests assessed by VeVA Core MN dedicated CAB	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
VeVA Core MN Release & Deployment Management ²	Volume of VeVA Core MN Change Requests validated by VeVA Core MN Release & Deployment Manager	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
ARF MN Change Management	Volume of Changes assessed by ARF MN dedicated CAB	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
ARF MN Change Management	Volume of Emergency Change Requests assessed by ARF MN dedicated CAB	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
ARF MN Release & Deployment Management	Volume of ARF MN Change Requests validated by ARF MN Release & Deployment Manager	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR
Exercises Continual Service Improvement	Volume of CSI items managed in Exercises CSI register	Minimum Frequency: monthly to Customers SME; Summary and exceptions at the QSLR

Standard Service Support Levels:

N/A

¹ VeVA Core MN Change Management currently not funded within this service

² VeVA Core MN Release & Deployment Management currently not funded within this service

Service Cost / Price:

This is an organic (enabling) service. Organic meant that the cost is distributed across all services in the catalogue that benefit from SMC Features. Distribution occurs through a “weighted” matrix. The weight is proportional to the consumer-service value and the quantity of features leveraged by that service.

OTH004 DCIS – Management Support Service

Service ID: OTH004

Service Name: DCIS – Management Support Service

Portfolio Group: Other Services

Service Description: The Service provides Operations Planning and Service Management (OPSM) support to the customer, as well as the primary NCI Agency interface and initial point of contact with the customer for in year execution of the services in accordance with agreed standards within the Service Level Agreement (SLA). The Service entails the management and coordination of all Deployable Services that are delivered to the service consumer at each of their peace time locations.

Value proposition: The Service provides management and reporting of all services, providing confidence to the customer that services delivery will continue as described in the respective SLA.

Service Features: The Service has the following features:

- Service monitoring, measuring, and Quality reporting, as defined in the SLA including Quarterly Service Level Reports;
- Availability Management Quarterly Service level Report (QSLR);
- Change Management Plan, Monthly update;
- Obsolescence Management, Quarterly Report on End of Life (EoL) of software and/or hardware;
- Service Delivery Schedule (Mid-Term and Short-Term Planning and coordination of Preventive Maintenance Activities (PMI), Advanced Schedule Interventions (ASIs), and Minor and agreed Major Changes);
- Transition Management for projects that are in support of the customer, but funded through the NATO Security and Investment Program (NSIP);
- Customer Account Management to supplement, but not replace, existing processes, for example: Customer Request Form (CRF) and related Price Proposal/ Purchase Order tracking, Exercise/ Operational planning, SLA Development, etc.
- Completion reports after each scheduled maintenance activity.

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service prerequisites: None

Standard Service Support Levels: N/A

Service Cost / Price: The Service is costed as an underlying service within each DCIS service (INF020, INF035, INF036, INF037, INF040, INF044).

WPS008 Enterprise Services Operations Centre

Service Name: Enterprise Services Operations Centre (ESOC) Service

Portfolio Group: Underlying Service

Service Description: The Enterprise Service Operations Centre (ESOC) operates as the 24/7 Single Point of Contact (SPOC) for all in-service support aspects of NCI's services. It plays a critical role in enabling operational readiness for Static Warfighting Headquarters, Alliance Operations and Missions, Exercises, and services to Nations and other customer organizations. By maintaining continuous monitoring, control and reporting functions over the NCI Agency's CIS infrastructure and services, ESOC ensures network integrity and end-to-end service coherence through the consistent application of enterprise processes. The service provides Level 1 and Level 2 support on IT incidents, Service requests, Requests for Information (RFI) and Change requests for all NCI Agency provided services. The service also offers monitoring and coordination of Level 3 support that is provided with the escalation of Level 1 and Level 2 raised incidents on the Static and Deployable infrastructure to Business Areas (BA) and Vendor. ESOC ensures efficient IT incident, Service Request, Request for Information and Change Request management and resolution and maintains continued situational awareness through comprehensive reporting.

Value Proposition:

- **Service Reliability and Uptime:** Applying established service management practices to reduce the impact of outages and maintain consistent performance to meet user values and service resolution targets from standing Agreements. The Service provides continuous monitoring, response, control, and operational reporting capabilities for the NCI Agency's operated CIS infrastructure and services to support network integrity and end-to-end service delivery coherence.
- **Issue Prevention and Early Alerts:** Furthermore, the Service enhances the ability to avoid IT services degradations and/or interruptions minimizing the impact on User Communities by proactively taking actions on identified disruptive service events. Leveraging monitoring tools, alerts, alarms and warnings, key service indicators to detect and address risks before they affect users. All IT incidents will be assigned with the resolution priority agreed with the Customer (i.e. ABIPAT).
- **Coordinated Incident Management:** Managing incidents in real time with dedicated teams, and with Agency business areas (BAs) and Deployable Network Operation Centre (DNOC) ensuring quick resolution and minimizing disruption.
- **Clear Reporting and Communication:** Supporting transparency through structured updates, reports, and defined escalation channels. The full range of the Agency's support capabilities will be available via a single point of contact being the ESOC DO, which serves as key stakeholder on maintaining strong liaison with customer communities in order to resolve Incidents prioritization conflicts, coordinate service outages and escalate / notify hierarchically and functionally critical incidents as deemed necessary and agreed-upon.
- **Effective Use of Resources:** Using staff and tools where they are most needed using a tiered support structure and clear prioritization. The Service provides efficiencies in terms of overall costs of service delivery and reducing Incident/Service Request resolution times through centralized management.

- **Fulfil Service Delivery Targets:** Sustained by mature ITIL Service Operations best practices, the Service enables the exercise of the command and control over all service assets ensuring service delivery is in accordance with all contracted service provisioning agreements (SLAs, SSPs, MOUs, POW, etc.).

Service Features: Operating 24/7, ESOC delivers the following key service features:

- **Single Point of Contact (SPOC):**
Single point of contact between the service provider and the users or customers for what concern services disruptions, services requests, request for information, also some categories of change requests (up to CAT2). This feature is eased by the establishment of a single telephone extension enabling Users and Customers across NATO to benefit from full range of the Agency's support capabilities via a single point of contact and gain efficiency in terms of overall costs and Incidents / Service Requests resolution time.
- **Request for Information (RFI) Management:**
The centralized Service function enables the possibility to request and receive information about service requests and their status, provide an interface for other activities such as customer change requests, maintenance contracts, SLM, service asset and configuration management, availability management, IT service continuity management and assist with general information, complaints or comments.
- **Duty Officer (DO) Team:**
The ESOC Service enables the command and control node in the function of the DO Team, making decisions in real-time regarding disposition and employment of NATO's C4ISR assets, within the constraints provided by political, legal and contractual direction. The Duty Officer (DO) Team supports the Service to execute this function by having an Officer on duty at all times, 24/7/365. DO is also responsible to maintain the liaison with designated customers representatives and the DNOC in order to provide situational awareness and de-conflict cross-customer operational priorities. Duty Officer Team play also an active role by implementing the proper levels and timescales in functional and hierarchical escalation of incidents, Major incidents, problems and customers' complaints.
- **IT Incidents Management:**
ESOC Service is responsible for the lifecycle management of IT incidents of all NCI Agency Services with the aim to restore as quickly as possible unexpectedly degraded or disrupted services to users and minimize impact to operations. Incidents may be recognized by technical staff, detected and reported by event monitoring tools, communications from users (usually via a telephone call to the service desk), or reported by third-party suppliers and partners. ESOC ensures that incident management activities support agreed service levels from standing Agreements (SLA, SSP, MOA, TOA) and other relevant agreements (i.e. CISSUPPLAN from Exercises and Missions) and objectives by prioritizing those activities based on actual operational need. Service assists Service Level Management (SLM) teams on Agency and Customers' side to define measurable responses to service disruptions and to review SLAs objectively enabling to determine the actions necessary as part of the Agency's Continuous Service Improvement (CSI) process and service improvement plan (SIP), where required. IT Incident management also covers following sub-features:

- **Multi-Tiered Support Model** – Structured support tiers with clear escalation pathways, ensuring rapid incident resolution across the full lifecycle of IT incidents and service requests.
- **Management of High-Priority Incidents** – Dedicated Duty Officers (DOs) lead the response to high and critical incidents, facilitating proactive communication, coordinated resource allocation, and minimized downtime.
- **Incident Coordination** – Dedicated team managing the incident management lifecycle by coordinating the detection, classification, resolution, and post-incident analysis, ensuring cross-team collaboration, managing resources effectively, and supporting continuity during disruptions.
- **Transparent Reporting & Escalation** – Comprehensive reporting mechanisms and well-defined escalation protocols ensuring accountability, visibility, and informed decision-making.
- **Service Requests Management:**
ESOC Service is responsible for the lifecycle management of all Users' generated service requests. Listed below the value this Service feature brings to Users:
 - Ability to provide quick and effective access to standard services that operations staff can use to improve their productivity;
 - Ability to effectively reduce the bureaucracy involved in requesting and receiving access to existing or new services, thus also reducing the cost of providing these services;
 - Ability to increase the level of control over requested services through a centralized fulfilment function. This in turn can help reduce the cost of support.
- **Network Monitoring and Events Management:**
ESOC Service manages Network and monitored IT infrastructure events throughout their lifecycle to include the coordination activities to detect events, make sense of them and determine the appropriate control, response and escalation actions. Listed below the indirect Service feature benefit:
 - Provides mechanisms for early detection of incidents. In many cases, it is possible for the incident to be detected and assigned to the appropriate group for action before any actual service outage occurs.
 - Makes it possible for some types of automated activity to be monitored by exception – thus removing the need for expensive and resource-intensive real-time monitoring, while reducing downtime.
 - Provides recommendations for automated operations, thus increasing efficiencies and allowing expensive human resources to be effectively used.
 - Has a direct bearing on service delivery and customer satisfaction.

Service Flavours:

The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret.

Service prerequisites: None

Standard Service support levels: The ESOC Service is available 24/7.

Available hours	First Call Resolution	Target Time to Pick Up
24/7 ⁽¹⁾	75%	• 75% ≤ 20s • 80% ≤ 30s • 85% ≤ 60s

⁽¹⁾ Outside the working hours, during the Weekends and NATO Holidays, the Enterprise Service Operations Centre is available 24/7 with same quality targets assuming that the Customers' call volume and Services support demand is reduced. Any exceptions on Service demand outside the "Customer's working hours" (ex: Exercise Support, Ministerial, etc.) as well as to Service Level Targets are subject to a Price Proposal (PP).

Service Cost / Price: The cost of WPS008 is covered under NDW001, NDW002 and WPS006.

Annex B - Non-Standard Customer Services

OTH008 Support to Customer's Operational Mission and Business Continuity Plans (BCPs)

Service ID: OTH008

Service Name: Support to Customer's Operational Mission and Business Continuity Plans (BCPs)

Service Type: Customer facing

Portfolio Group: Other Services

Service Status: Available¹

Service Description: The OTH008 - Support to Customer's Operational Mission and Business Continuity Plans (BCPs) service covers activities provided in direct support to the customer's day-2-day operational mission or direct support provided to their Business Continuity Plans (BCP) either being planned or already in place.

Example activities are preventive maintenance (periodically functionality checks, updates, etc.) on BCP assets on stock, execution of the Business Continuity Plans, operating from alternative/multiple locations, moving equipment between alternative locations, etc.

Value Proposition: The service accounts for the direct local support required stemming from specific customer requirements related to their operational mission and/or their specific Business Continuity Plans that is either not accounted for in the standard catalogue services or through any other activities/projects. This includes financial activities in support of operational requirements (e.g. procurement of small value assets) or urgent support required to minimize operational disruptions.

Service Features: Detailed list of activities will be documented in the respective Service Level Agreement (SLA)/Service Support Package (SSP) which will guarantee availability of the resources required to provide the support.

Examples of activities covered under the service includes (non-exhaustive list):

Procurement/Vendor Management activities:

- Procurement of small value assets as detailed in the External CIS section of the customer's SLA/SSP (or the price proposal if service is requested via the Customer Requirements Form (CRF) process)
- Contractual efforts required in managing outsourced CIS service contracts,

Business Continuity Plan activities:

- Participation and technical support required for creation/amendment of customer BCPs, any amendment of NCIA recovery plans required to fulfil Customer's BCPs and in the execution and/or exercising of customer's Business Execution Plans
- Periodical check of BCP assets on stock including operational checks and preventative maintenance activities

¹ Service Description will be further refined and enhanced in 2026 supporting full alignment between in-service support activities, customer agreements and associated cost

- Relocation of support staff to different operational location if required by operational context/situation

Service Request: NATO Entities shall include their requirements into the respective Service Level Agreement (SLA)/Service Support Package (SSP) under Annex 14 - Other services.

For non-SLA/SSP customers the support arrangements shall be covered via the Customer Requirements Form (CRF) process.

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service Prerequisites: N/A

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is Per Defined Service. Cost for each defined service is individually set up, in accordance with agreed local scope and conditions of the service delivery, as well as valid NCIA Customer Rates.

OTH009 Enhanced Local Support

Service ID: OTH009

Service Name: Enhanced Local Support

Service Type: Customer facing

Portfolio Group: Other Services

Service Status: Available¹

Service Description: OTH009 - Enhanced Local Support, covers local support requirements that are not already accounted for in standard catalogue services and/or covered by the Incident Response Readiness Team (IRRT). This can for example, be support to local Customer's prioritised baseline activities, events and current operations (onsite and offsite) that require periodic or continuous enhanced service support with increased operational focus and readiness enabling enhanced response and restoration targets during and/or after the standardised business hours.

Value Proposition: The service accounts for the Customer's requirements for enhanced support over and above the baseline already being included in the standard service rates for standard services.

Service Features: Detailed list of supported services and the enhanced support requirements (including KPIs) will be documented and resourced in the respective Service Level Agreement (SLA)/Service Support Package (SSP).

Examples of activities requiring enhanced support (non-exhaustive list):

- Periodic service support with increased operational focus and readiness enabling enhanced response and service restoration targets to support Customer's prioritised baseline activities, events and current operations (onsite and offsite).
- Continuous service support with increased operational focus and readiness enabling enhanced response and service restoration targets to support Customer's prioritise baseline activities, events and current operations (onsite and offsite).
- Physical presence of a local service desk function, etc.
- Enhanced support to Customer catalogue services over and beyond what is included in the service offerings.
- Single Point of Contact function for customers operating at multiple geographical locations that otherwise will be supported by multiple NCIA CIS Support Units (CSUs).

Service Request: NATO Entities shall include their requirements into the respective Service Level Agreement (SLA)/Service Support Package (SSP) under Annex 14 - Other services.

For non-SLA/SSP customers the support arrangements shall be covered via the Customer Requirements Form (CRF) process.

Service Flavours: The Service is available as a single flavour.

¹ Service Description will be further refined and enhanced in 2026 supporting full alignment between in-service support activities, customer agreements and associated cost



Available on: Defined in SLAs / SSPs

Service Prerequisites: N/A

Standard Service Support Levels: Defined in SLAs / SSPs

Service Cost / Price: The unit of measure for the Service is Per Defined Service. Cost for each defined service is individually set up, in accordance with agreed local scope and conditions of the service delivery, as well as valid NCIA Customer Rates.

OTH010 Campus ICT Services

Service ID: OTH010

Service Name: Campus ICT Services

Service Type: Customer facing

Portfolio Group: Other Services

Service Status: Available¹

Service Description: The OTH010 - Campus ICT service covers for local office reallocations, operating standard technical facilities (technical rooms, equipment rooms, etc.), support to local cabling as well as supporting Host Nation building maintenance tasks, such as controlled facility shutdown. Maintenance of local configuration management database (L-CMDB) is also included under the Facility Management service.

NOTE: Any activities related to the central configuration management database (CMDB) is excluded and covered by OTH001 - Service Management and Control Function service.

Value Proposition: The service accounts for various support provided to the local facilities which is not already covered by the territorial Host nation or via other Real Life Support (RLS) arrangements in place.

OTH010 - Facility Management also accounts for the physical relocation NCIA assets in periods with office moves, larger reallocation of staff and usage of temporary buildings, etc.

Note: The service only accounts for the activities that are not already included in the standard service rates. Replacement, configuration and installation of faulty assets etc. are covered under standard service rate and hence not included here.

Service Features: Detailed list of activities will be documented in the respective Service Level Agreement (SLA)/Service Support Package (SSP) which will guarantee availability of the resources required to provide the support.

Examples of activities covered under the service includes (non-exhaustive list):

- Bulk reallocation of NCIA assets during period of planned office moves or reallocation of customer staff
- Supporting Host Nation or Customer's building maintenance tasks affecting ICT service delivery (controlled facility shutdown, building cabling infrastructure works and projects, power supply and cooling/air-conditioning works and projects etc.)
- Provisioning of and/or support to ICT services required on Campus such as equipment racks, power distribution units within equipment racks, access control systems, CCTV cameras, Digital Signage Systems, emergency notification systems, etc.
- Multiple locations support within Geographical Area of Responsibility

Service Request: NATO Entities shall include their requirements into the respective Service Level Agreement (SLA)/Service Support Package (SSP) under Annex 14 - Other services.

¹ Service Description will be further refined and enhanced in 2026 supporting full alignment between in-service support activities, customer agreements and associated cost



For non-SLA/SSP customers the support arrangements shall be covered via the Customer Requirements Form (CRF) process.

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service Prerequisites: N/A

Standard Service Support Levels: Defined in SLAs/SSPs

Service Cost / Price: The unit of measure for the Service is Per Defined Service. Cost for each defined service is individually set up, in accordance with agreed local scope and conditions of the service delivery, as well as valid NCIA Customer Rates.

OTH011 Local Exercise Support

Service ID: OTH011

Service Name: Local Exercise Support

Service Type: Customer facing

Portfolio Group: Other Services

Service Status: Available¹

Service Description: The OTH011 - Local Exercise Support combines the activities currently listed in SLA Annex 15 (Support to Exercises) with the previous LEG008 activities covering localized aspects related to exercises. Examples are management and configuration of Interface with Nations Module (INM) or participation in weekly and ad-hoc planning meetings related to exercise calendar. OTH011 also accounts for exercise support to non-common funded customers (via CRF process) and for exercise participants that are not covered by the scope of Centralized SLA (CSLA) supported exercises.

Value Proposition: The service provides customers that are not covered under Centralized SLA (CSLA) exercise efforts with the ability to plan and schedule NCIA support for local participation in exercises and in support of the associated exercise planning required.

Note: Direct technical support to customers' permanent Education and NATO Education, Training, Exercises and Evaluation (ETEE) Environments are covered under OTH012 - Unique (local) Capabilities.

Service Features: Detailed list of activities will be documented in the respective Service Level Agreement (SLA)/Service Support Package (SSP) which will guarantee availability of the resources required to provide the support.

Examples of activities covered under the service includes (non-exhaustive list):

- Planning of the CIS support for all exercises, events, workshops and conferences as per Annex 15 of SLA/SSP
- Requirements assessment and analysis
- Participation in all required planning events, Customer Meetings, conferences and technical meetings
- Providing Subject Matter Expertise (SME) support, advising and recommending technical solutions.

Service Request: NATO Entities shall include their requirements into the respective Service Level Agreement (SLA)/Service Support Package (SSP) under Annex 15 - Local Exercise Support .

For non-SLA/SSP customers the support arrangements shall be covered via the Customer Requirements Form (CRF) process.

Service Flavours: The Service is available as a single flavour.

¹ Service Description will be further refined and enhanced in 2026 supporting full alignment between in-service support activities, customer agreements and associated cost



Available on: Defined in SLAs/SSPs

Service Prerequisites: N/A

Standard Service Support Levels: Defined in SLAs / SSPs

Service Cost / Price: The unit of measure for the Service is Per Defined Service. Cost for each defined service is individually set up, in accordance with agreed local scope and conditions of the service delivery, as well as valid NCIA Customer Rates.

OTH012 Unique (local) Capabilities

Service ID: OTH012

Service Name: Unique (local) Capabilities

Service Type: Customer facing

Portfolio Group: Other Services

Service Status: Available¹

Service Description: The OTH012 - Unique (Local) Capability groups together all other capabilities at customer locations that are not covered under the standard catalogue services and hence are considered non-standard local capabilities where the customer requires support from NCIA.

The uniqueness of the customer's operational mission and the geographical locations they operate in demands for the ability to obtain specialized and localized annual support from NCIA.

The service also accounts for direct technical support to customer's local Education, Training, Exercises and Evaluation Environments (ETEEs).

Value Proposition:

The OTH012 - Unique (local) Capabilities service accounts for the direct local support required to support the specific capabilities at customer locations. The service also accounts for dedicated support to capabilities that are undertaken the process to be included as a standardized catalogue service (i.e. in the 'pipeline' service status).

Each unique (local) capability will be detailed with its separate ID allowing for full transparency and traceability.

Service Features: Detailed list of activities will be documented in the respective Service Level Agreement (SLA)/Service Support Package (SSP) which will guarantee availability of the resources required to provide the support.

Examples of activities covered under the service includes (non-exhaustive list):

- Support to Application services not covered by CCSC
- Support to Customer's Unique Business processes
- Support to NATO Enabled Partner Infrastructure (NEPI) pipeline service
- Support to Electronic Key System (EKS) Connectivity
- Support to External Communication Lines Filtering capabilities
- Support to Public Announcement (PA) Systems or local Audio/Visual capabilities
- Support to Customer's ETEE environments and associated technical facilities

Service Request: NATO Entities shall include their requirements into the respective Service Level Agreement (SLA)/Service Support Package (SSP) under Annex 14 - Other services.

¹ Service Description will be further refined and enhanced in 2026 supporting full alignment between in-service support activities, customer agreements and associated cost



For non-SLA/SSP customers the support arrangements shall be covered via the Customer Requirements Form (CRF) process.

Service Flavours: The Service is available as a single flavour.

Available on: Defined in SLAs / SSPs

Service Prerequisites: N/A

Standard Service Support Levels: Defined in SLAs / SSPs

Service Cost / Price: The unit of measure for the Service is Per Defined Service. Cost for each defined service is individually set up, in accordance with agreed local scope and conditions of the service delivery, as well as valid NCIA Customer Rates.

SME006 Operational Analysis Service

Service ID: SME006

Service Name: Operational Analysis Service

Portfolio Group: Subject Matter Expertise Service

Service Description: Operational Analysis (OA) is a consultancy service, which consists of developing and applying fit-for-purpose approaches and scientific methods to analyse problems across the spectrum of defence activities, and supporting decision makers in understanding, visualising and resolving them.

Value Proposition: The OA service helps decision makers within NATO and the Nations to make better informed decisions based on evidence. This service offers reliable and timely expert support to decision makers in NATO and Nations. Professional analysts, who have an excellent understanding and extensive experience in defence and security issues, supported by analytical supporting tools (e.g. models) and techniques (e.g. wargaming, data science), are able to help scoping an issue that decision makers face and provide objective analysis of available options, leading to better informed decision making. The OA experts have decades of involvement in defence planning support, OA support to Alliance Operations and Missions, and support to peacetime and operational Headquarters. They also have a proven track record of delivering high quality expertise and products to customers' satisfaction, on time and within budget.

Service Features: NCI Agency can provide ad hoc and flexible Operational Analysis consultancy to NATO and Nations through the application of tailored analytical methods to solve complex problems as typically faced by organisational leaders and operational commanders. The Service can provide support in a range of fields such as the following (non-exhaustive list). Of note, the support and techniques described here can also be applied in other context.

- **Defence Planning:** provision of a full spectrum of technical consultancy, analysis and advice to support NATO and the Nations in Defence Planning (DP), primarily with focus on support to the NATO Defence Planning Process (NDPP). It includes (non-exhaustive list):
 - Analytic expertise in support of the NATO Defence Planning Process (NDPP) activities, including identification of capability requirements, apportionment of requirements, and suitability and risk assessment; this analytic support involves for instance:
 - Development of new methodologies;
 - Analysis, including very large data sets, through a range of modelling techniques and tools;
 - Development of representative scenarios;
 - Structured mission analysis (mission-to-task decomposition);
 - Assessment of risk and aggregation techniques;
 - Support to assessing burden sharing in terms of relative costing techniques;

- Application of OA techniques to facilitate decision making;
- Provision of subject matter expertise (SME) across military and non-military domains, including reach to extensive networks of SMEs across NATO and in the nations;
- Analytic expertise in support of national Defence Planning activities, such as:
 - Education and mentoring with NATO analytic approaches;
 - Facilitation and delivery of customised Defence Planning studies;
 - Access to and development of analytic supporting tools and models (e.g. the Joint Defence Planning Analysis and Requirements Toolset (JDARTS));
 - Support to implementation of robust national capability-based planning processes;
 - Exploitation of established NATO best practice, tailored to fit national needs;
 - Facilitation of the use of NATO DP tools & models.
- **Support to Headquarters (peacetime & operational):** provision of tailored analytical support to tactical, operational and strategic-level HQs within Nations and the NATO Command and Force Structures, during peacetime and/or crisis situations. This support includes areas such as:
 - Wargame development and facilitation;
 - Support to planning activities such as Course of Action analysis, support to concept development activities, lessons identified;
 - Operational assessment, battle information management, data analysis (time-series, geospatial, survey), and streamlining of existing HQ data collection/analysis processes, implementation of advanced analytical techniques (mathematical modelling and optimisation algorithms);
 - Organisational design and improvement of processes, including analysis of 'as-is' processes and provision of 'to be' structures or changes;
 - Support to analysis of information exchange requirements, and modelling of processes and information flows.

This support is available on-site (static or deployed locations) or as remote, reach back arrangement.

- **Operational and User Requirements:** provision of expertise to support, through exploitation of products and knowledge from any of the other OA services, a range of areas including:
 - User requirements capture and validation;
 - Mentoring in the employment of NATO Functional Area Services (FAS) to meet military business process and information exchange requirements;
 - Business decision support e.g. development of NATO FAS Lifecycle Roadmap;
 - IT procurement and training decision support e.g. development of dashboard highlighting technology employment/retirement and deprecation;
 - Gap analysis to enable the integration of NATO processes to ensure a seamless "end-to-end" approach to capability delivery and sustainment.
 - Support to architecture development.

Service Flavours: The OA service is tailored to meet individual needs of a customer.



Available on: N/A

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost/ Price: The unit of measure for the Service is Per Defined Service. Cost for each defined service is individually set up, in accordance with agreed scope and conditions of the service delivery, as well as valid NCI Agency Customer Rates.

SME011 Subject Matter Expertise and Technical Consultancy Service for NATO Software Tools (NST) Communications and Information (C&I) Partnership

Service ID: SME011

Service Name: SME and Technical Consultancy Service for NST C&IP

Portfolio Group: Subject Matter Expertise Services

Service Description: NST C&IP provides Participants with SME and Technical Consultancy services for evolution of programme of work including incorporation of new operational requirements, building and/or acquiring new tools, collection and management of NST C&IP related functional service and support requirements for subsequent years' Programme of Work.

Based on this service provision for participant Nations, NST C&IP is experienced to advise requestors, primarily the potentially joining Nations, on the best use of a wide range of NCI Agency services related to applications, to meet their specific business requirements and achieve their business objectives (See service features).

Value Proposition: For provision of these services, NST C&IP POW leverages on the experience and accumulated knowledge of NST C&IP and other NCI Agency teams supporting NATO Nations and organizations to align with the NATO technological vision and NCI Agency processes.

NST C&IP core team evaluates the service request and provides support on NCI Agency processes, legal, contractual and IPR issues of NATO FASes usage for national purposes. If the service request is related to the applications and business processes themselves, SMEs of specific systems and processes are involved. If the service request is related to infrastructure, request is forwarded to teams with in-depth knowledge on infrastructure.

Service Features:

- Provision of remote SME support on NCI Agency processes
 - 1.1 SME support for Request for Information(RFIs) on NCI Agency processes such as acquiring access to EDML, joining a partnership, and submitting a CRF.
- Provision of remote SME support on legal, contractual and IPR issues and constraints with utilization of NATO FASes for national purposes
 - 2.1 SME support for RFIs on current status and initial analysis towards the resolution of issues
- Integration of C5ISR¹ IT systems related to NATO FASes

¹ Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance

3.1 Remote SME support for RFIs on new solutions and their feasibility and cost analysis for way ahead

- Achievement of increased effectiveness in usage of NATO FASes to manage business processes

- 4.1 NST C&IP FAS Overview training on-site
- 4.2 On-site SME support for implementing national processes via the usage of NATO FASes
- 4.3 Provision of initial feasibility and cost analysis for business process interoperability between NATO and national tools
- 4.4 On-site SME support for RFIs on new business solutions and their feasibility and cost analysis

- Resolution of infrastructure and NATO/Nation network boundaries issues and architectural changes affecting workability with NATO FASes

- 5.1 Provision of one service request for changing the existing network configuration
- 5.2 Provision of remote SME support for addressing potential solutions and cost estimates for wider service request

- NATO FASes application lifecycle transformation including the adoption of current and new technology, methodologies and processes such as DevOps¹, Microservices², Containerization³ and Cloud Technologies⁴

- 6.1 Provision of on site knowledge transfer session on new technologies:
- 6.2 Remote SME Support for effective usage of new technologies within the Nation:

- Determination of strategy for the way ahead
- Stakeholders analysis

- Inclusion of national requirements in NATO Applications in the NST C&IP POW toolset mainly via the provision of support for:

- 7.1 Requestor representatives in Change Control Boards (CCBs) and Operational User Groups (OUGs)
- 7.2 Formulation of one user requirement or change request for inclusion

¹ DevOps is a culture that promotes collaboration between Development and Operations Team, which allows deploying code to production faster, and in an automated way.

² Microservices are a software development technique—a variant of the service-oriented architecture (SOA) architectural style that structures an application as a collection of loosely coupled services.

³ Container is a standardized unit of software which isolate component from its environment and ensure that it works uniformly despite differences for instance between development and staging. NST C&IP provides containerization support to develop a common understanding of containerisation strategy and to analyse how best to exploit containerisation for the NATO FASes.

⁴ Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

7.3 End-to-end monitoring and reporting on the change management processes

Service Flavours:

Remote support - Available
On-site support – Available

Available on: Any network of customer subject to security requirements of specific FAS application

Service Prerequisites: None

Standard Service Support Levels:

Service Availability: *The service is available during standard business hours.*

Ticket can be raised via NST C&IP Inbox 24/7 however the NST C&IP Support availability is:

Availability Target
Business Hours Mon-Fri 08:30 – 17:30

Service Restoration: N/A

Service Cost / Price: Cost for each defined effort is individually calculated, in accordance with agreed scope and conditions of the service delivery, as well as valid NCI Agency Customer Rates.

References:

- NST C&IP 2020 POW and Appendices
- CIP General Rules, 08 Dec 2015
- NST CIP Partnership Arrangement, 12 Oct 2016

SME013 Single European Sky Air Traffic Management Research (SESAR) Capability Implementation Study

Service ID: SME013

Service Name: SESAR Capability Implementation Study

Portfolio Group: Subject Matter Expertise Service

Service Description: This Service utilizes NCI Agency Subject Matter Expertise (SME) to identify the impact of the Single European Sky (SES) initiative on the AirC2 systems used in NATINAMDS, to analyse, identify, validate solutions and identify to which extend and by when the AirC2 systems under the AirC2 Governance will have to be adapted.

The Single European Sky (SES) is an initiative launched by the European Commission (EC) to reform the architecture of European Air Traffic Management (ATM). The key objectives of SES are to restructure the European Airspace as a function of air traffic flows, to create additional capacity and to increase the overall efficiency of the ATM system. The SESAR programme is the “technical pillar” to achieve the SES objectives by modernising the ATM of civil aviation in Europe. The SESAR Deployment Programme (DP) has introduced new concepts resulting from the SESAR research.

In 2016 and 2018, ACT conducted two initial studies, which focused on possible improvements to ACCS to cope with upgrades introduced by SESAR 1 Research Programme (2008-2016).

These studies will continue into identification and validation of requirements for upgrading NATO and National AirC2 Systems to remain interoperable with ATM and Air Traffic Control (ATC).

Value Proposition: This service combines NCI Agency SME holding AirC2 system expertise with information and background information available through liaison with EUROCONTROL as necessary to identify and validate the impact of SESAR on the NATINAMDS.

Service Features: This expert matter Expertise Service will complete the studies, analyse the SESAR DP and timelines, analyse and identify potential impact from SESAR, develop, prototype and validate potential solutions and propose change requests for affected AirC2 systems together with a necessary implementation timeline or roadmap.

The service is aimed at advising SHAPE as the main customer and the AirC2 governance on required action, priorities and timelines to stay compatible ATM/ATC when SESAR will be rolled out.

Service Request: Service should be requested through a CRF, or by a SLA/POW

Service Flavours: The service is provided as a singleton service through the AMDC2 ISS POW.

Available on: N/A

Service Prerequisites: N/A

Standard Service Support Levels: N/A



Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions between NCIA and SHAPE on an annual basis via AMDC2 ISS POW.

FMN001 Provision of Support to the Federated Mission Networking (FMN) Framework

Service ID: FMN001

Service Name: Provision of Support to the Federated Mission Networking (FMN) Framework

Portfolio Group: Other

Service Description: This service provides:

- Support to the ACO funded portion of the management and working group structures that support the direction and development of the FMN Framework. [SLIN13.1]
- Support to derisking of the implementation of federated capabilities through collective and federated CIAV testing with Nations Affiliated with the FMN Framework.

Value Proposition: With NAC approval of NFIP Vol 1 on 29 January 2015, NATO committed itself to be the key contributor to and facilitator of the FMN Framework. ACO, ACT and IMS provide annual funding to NCI Agency to provide SME to support their respective responsibilities within the FMN Framework. This service is to maintain ACO's portion of the NATO funded support to the FMN framework and its organizational structure, as directed by the MC and subsequently approved by the NAC. The maintenance of ACT's portion of the NATO funded support to the FMN framework and its organizational structure is funded via the ACT POW. The support provided to help ACO represent the NATO Command Structure as an Affiliate to the FMN Framework (NCSaaA) is provided via FMN002.

Service Features:

- **Support the FMN Secretariat**
 - a. Provision of Change and Implementation Coordinator within the FMN Secretariat in accordance with the NAC approved FMN Implementation Plan (C-M(2015)0003-AS1) and the Military Committee FMN Transition Plan (IMSM-0093-20015) in order to:
 - (1) Provide CIC Working Group (WG) representation in FMN Secretariat, managing routine, day-to-day CIC WG activities. The primary tasks of the FMN Secretariat representative (CIC WG Coordinator) are information exchange with the FMN Secretariat members, interaction with other FMN WG Secretariat representatives and supporting the Chairperson with routine and day-to-day CIC WG activities;
 - (2) Provide experience in coordination of change management of complex military C4ISR systems to a deployed military force;
 - (3) Provide a broad expertise on understanding of military capabilities / systems / services and their inter-relationships;
 - (4) Provide a good understanding of the support provided by such systems to military business processes;
 - (5) Provide coordination on FMN Baseline-wide changes through the system, ensuring traceability of requirements, checking completeness of release

documentation and verification and validation results, and associated artefacts;

- (6) Provide guidance and policies to FMN Affiliates to submit Request for Change (RFC) to the FMN Change Advisory Board (CAB);
- (7) Provision of FMN Community of Interest (COI) Portal CIC WG section update, maintenance, monthly sanity check; publication and dissemination of CIC WG's Information and relevant products;
- (8) Provision of CIC WG's Tasks Tracking and Updating (monthly activity);
- (9) Provision of CIC WG weekly report to FMN Secretariat weekly update. Attendance to weekly internal meetings;
- (10) Provision of CIC WG monthly report to FMN Secretariat monthly update;
- (11) Provision of coordination, support and attendance for FMN Management Group (MG) Meetings (2x Year). Contribution to Preparation, Information Briefs, Decision Briefs, agenda, content, meeting execution, record production;
- (12) Provision of coordination, support and attendance for FMN MG Preparation Meetings (2x Year). Contribution to Preparation, Information Briefs, Decision Briefs, agenda, content, meeting execution;
- (13) Provision of Coordination for FMN CIC WG Meetings (4x Year). Preparation, calling notice, agenda, content, meeting execution, minutes coordination (quarterly);
- (14) Provide FMN Secretariat newcomers induction training, CIC WG 101 Briefing (annually);
- (15) Provide coordination and standardization criteria and policies for FMN Kanban Dashboard Management (RFCs Management, FMN Baseline Management);
- (16) Provide coordination and chairing for the CAB (twice per month);
- (17) Provide, for FMN Management Directive, coordination and support for WGs / Architecture Coordination Body (ACB) and FMN SEC LO review (Mainly FMN CIC WG TORs Update, contribution) (annually);
- (18) Provision of coordination and guidance for FMN CIC WG deliverable products production and maintenance:
 - (a) FMN Framework IT Service Management Documents Update;
 - (b) FMN CIC WG Standard Operating Procedure (SOP) Change Management;
 - (c) Kanban Dashboard User Guide (SOP) and 101 Brief;
 - (d) JMEIs;

- (e) CIS Planning Guide w/ Annexes;
- (f) CIC Contribution to the FMN MN Governance and Management Directive [Template];
- (19) Provision of Coordination and Liaison w/ other FMN entities:
 - (a) Updates to FMN MG Chairperson;
 - (b) Updates to FMN Secretariat Director;
 - (c) WGs Coordination;
 - (d) FMN Inter-Working Groups Syndicates (IWGs) contribution and coordination;
- (20) Provision of support to FMN Secretariat Activities (daily);
- (21) Provision of support to FMN Secretariat Tasks, providing comments to Documents contribution.
- b. Provision of FMN Architect within the FMN Secretariat in accordance with the NAC approved FMN Implementation Plan (C-M(2015)0003-AS1) and the Military Committee FMN Transition Plan (IMSM-0093-20015) in order to:
 - (1) Chair the FMN Architecture Coordination Body;
 - (2) Act as ACB facilitator to IWGs: The ACB facilitator directs the IWGs to coordinate their activities and outputs in order to delivery compliant and coherent architecture products, which can be reused by WGs, FMN Affiliates and other relevant NATO bodies (e.g. NCIA, DPC CaTs and CaPs);
 - (3) Support the FMN Framework Architecture and direct the effective and efficient development (identification, specification, implementation, verification, and validation) of interoperable FMN capabilities across the WGs;
 - (4) Conduct weekly reviews of architecture issues, concerns and opportunities,
 - (5) Develop and maintain standardized "Ways-of-Working" for FMN architecture modelling, ensuring coherence, coordination and traceability of requirements;
 - (6) Align and Synchronize Architecture Activities to the FMN Battle Rhythm (lifecycle), aiding the synchronization of the FMN battle rhythm; increasing the speed and coherence of capability development;
 - (7) Coordinate the use of resources, facilitating the efficient use of architecture resources by providing a way to visualize priorities and maintain the ACB PoW;
 - (8) Optimize the (re)use of architecture products by maintaining the optimum way of exploiting architectural products across the FMN Framework;
 - (9) Establish and direct the FMN Architecture Management Structure;

- (10) Develop and maintain FMN architecture principles and guidance;
 - (11) Ensure alignment with NATO Architecture policies and directives by engaging and influencing the Digital Policy Committee (DPC) sub-structures and standards bodies and utilize the FMN Cooperative Arrangements;
 - (12) Engage FMN stakeholders to demonstrate the value of architecture and its use in the FMN Frameworks.
- c. Provision of unclassified COI FMN portal infrastructure to the FMN Secretariat for the governance and management bodies of the FMN initiative.
- **Support the FMN Operational Coordination (OC) Working Group**
 - a. The identification, development, and standardisation of Interoperability Operational Requirements (IORs), business processes, information exchange requirements, and operational/functional role-based minimum exchange requirement tables support the development of federated IT services needed to conduct subject expertise military procedures. This includes interdependencies with other procedures and services, and supporting architectures as required;
 - b. Procedural Instructions (PIs): The PIs, serving as the initial implementation point for cross-parameter understanding across all Affiliates (currently 40), are continually developed and incrementally improved as the process matures;
 - c. IOR Baseline: The identification, development, and prioritisation of Interoperability Operational Requirements, Security Requirements, and supporting Capability Enhancements across a broad range of operational procedures and technical services are divided into 21 capability areas (swimlanes). This is projected over 10 years, resulting in the annual deliverable of the IOR Baseline added to the 202X Update to the FMN Spiral Specification Roadmap;
 - d. Requirements of OC WG Facilitator: The OC WG Facilitator advises, directs, and maintains communication with IWGs, ensuring IWG Leads are engaged with the correct Programme of Works and aligned to priorities. Given that IWGs are Affiliate-driven and separate from the FMN, constant attendance by the Facilitator is necessary to ensure timely and accurate development of all required products;
 - e. FMN OC WG IOR Repository Management and Maintenance: The contractors are required to manage, maintain, and update the "OC WG FMN IORs Repository" in Tidepedia in accordance with approved procedures. This requirement is on an ad-hoc yet constant basis;
 - f. Issue Tracker for OC WG-assigned Issues: The OC WG ORMT contractors shall manage the Issue Tracker for OC WG-assigned issues. They are required to take action to resolve any issues where possible. If an issue cannot be resolved immediately, it must be presented to the OC WG Core team at the weekly meeting. All tasks are to be assigned to a person or organization to be handled in a timely manner and to the satisfaction of all concerned. If unresolved, the OC WG Core team must be informed of the reasons;
 - g. Alignment of OC WG and other FMN WGs through Liaison: Alignment of the OC WG with other FMN WGs is vital. The OC WG Core team has only one permanent position. The contractors provide continuity and consistency through constant

ongoing liaison, including attending other WG meetings and key events to provide OC WG input and views;

- h. Analyses Lessons Learned from exercises and Operations: Affiliates are required to notify through the LL and LI the secretariat and the OC WG all lessons learned or identified at the earliest opportunity. The contracted personnel are responsible for providing OC WG input and additional views.
- **Support the FMN Multinational CIS Security Management Authority (MCSMA) Working Group**
 - a. Provision of Cyber Security engineer / architect to the MCSMA WG and in attendance at WG meetings to develop and produce federated security documentation and products (e.g. Federated CIS Security Requirements, Technical and Procedural (SREQs), Security Reference Architecture and the templates for the Community Security Requirements Statements (CSRS), System Interconnection Security Requirement Statement (SISRS), the Statement of Compliance (SoC), the Approval to Operate (AtO), as it relates to each FMN Spiral Specification;
 - b. Provision of Cyber Security manager to the MCSMA to coordinate with NATO Cyber Security Capability Panels and Teams and workshops, in support of the approved FMN Cooperative Arrangement to include fulfilment of tasks received after the escalation of risks to the Military Committee (MC) regarding the misalignment between NATO Security Policies and FMN Goals;
 - c. Provision of Cyber Security engineer / architect to the MCSMA to check and ensure consistent integration of CIS Security requirements and products across FMN Framework bodies, including IWGs, and relevant products, such as FMN Spiral Security Requirements, Service Instructions, Procedural Instructions, Joining, Membership and Exiting Instructions (JMEIs) of each specific Spiral;
 - d. Provision of Cyber Security engineer / architect to the MCSMA WG to support alignment of MCSMA and FMN Framework repositories and data model, modelling conventions and artefacts across FMN Framework products;
 - e. Provision of Cyber Security Analyst to the MCSMA WG to produce the FMN Security Risk Assessment (SRA) using latest NATO PILAR tool.
- **Support the FMN Change and Implementation Coordination (CIC) Working Group**
 - a. Provide Naming and Registration Authority (NRA) for the FMN Framework to maintain ASN and IP Ranges assigned to the Affiliates and to respond to enquiries and help resolve conflicts;
 - b. Provide a CIC WG Change Management Administrator
 - (1) Provide managing in the FMN Change Management Process, which includes the FMN Baseline. A primary objective of this process is to ensure integrity and ensure quality control of the FMN Baseline. This is achieved using the CAB. In order for the CAB to function correctly, there is a tremendous amount of preparatory work that is conducted by the Change Management Administrator. Managing the change queue through the use of the RFC Kanban Board, Prioritizing RFCs in accordance with scheduled

AV&V events (CWIX, Exercises, ...) reviewing all Change request for accuracy and completeness prior to be submitted to the CAB, accurately documenting all records of change / decisions approved by the CAB ensuring an essential aspect of transparency and accountability in the change management process;

- (2) Provide support to CIC WG representation in FMN Secretariat, managing routine, day-to-day CIC WG activities. The primary tasks of the FMN Secretariat representative (CIC WG Coordinator) are information exchange with the FMN Secretariat members, interaction with other FMN WG Secretariat representatives and supporting the Chairperson with routine and day-to-day CIC WG activities;
- (3) Provide experience in change management of complex military C4ISR systems to a deployed military force;
- (4) Provide a broad understanding of military capabilities / systems / services and their inter-relationships;
- (5) Provide a good understanding of the support provided by such systems to military business processes;
- (6) Provide monitoring, tracking, and management on FMN Baseline-wide changes through the system, ensuring traceability of requirements, checking completeness of release documentation and verification and validation results, and associated artefacts;
- (7) Assist FMN Affiliates to submit RFC to the CAB, ensuring that all documentation is collated;
- (8) Develop the FMN Forward Schedule of Change with the CAB, taking into account operational requirements and Spiral Specifications;
- (9) Work with the NCI Agency's Head TMO on the assessment of the impact of NCI Agency and Affiliate induced changes to the FMN configuration of services. Where required, engaging with SMEs of NCI Agency. Provide a presence in the FMN Secretariat for Affiliate representatives to consult on FMN change management issues and general systems engineering issues;
- (10) Provision of tracking and updates of FMN CIC WG Affiliate's members Distribution List (Monthly update);
- (11) Provision of updated CAB WG Distribution (Monthly update);
- (12) Attendance to weekly FMN Secretariat Update internal meetings (Weekly Basis);
- (13) Attendance to weekly NCI Agency Enterprise Change Advisory Board (ENT-CAB) (Weekly Basis);

- (14) Provision of support and attendance for FMN MG Meetings (2x Year). Contribution to Preparation, Information Briefs, Decision Briefs, agenda, content, meeting execution, record production;
- (15) Provision of support and attendance for FMN MG Prep Meetings (2x Year). Contribution to Preparation, Information Briefs, Decision Briefs, agenda, content, meeting execution;
- (16) Provision of Support for FMN CIC WG Meetings (4x Year) Preparation, calling notice, agenda, content, meeting execution, minutes production and release (quarterly);
- (17) Provide coordination and support FMN CIC WG IKM Syndicate meetings (biweekly);
- (18) Provide material for FMN Secretariat newcomers' induction training, CIC WG 101 (annually);
- (19) Produce training material for Affiliates CIC WG National leads newcomers' induction training (annually);
- (20) Provide Daily Revision, Tracking, and Management of FMN Kanban Dashboard Management (RFCs Management, FMN Baseline Management);
- (21) Provide, for CAB Meetings, Preparation, Agenda, Record of Decisions, and Kanban Dashboard updates (twice per month);
- (22) Provision of support for FMN Management Directive, FMN CIC WG TORs Update, and contribution) (annually). Under guidance of FMN Affiliates and NCI Agency Service Strategy assist in maintaining the FMN Joining, Membership and Exit Instructions (JMEIs);
- (23) Provision of support for FMN CIC WG deliverable products production and maintenance:
 - (a) FMN Framework IT Service Management Documents Update;
 - (b) FMN CIC WG Standard Operating Procedure (SOP) Change Management;
 - (c) Kanban Dashboard User Guide (SOP) and 101 Brief;
 - (d) JMEIs;
 - (e) CIS Planning Guide w/ Annexes.
- (24) Provide CIC WG's Information Knowledge Management. Many of the FMN products that the CIC WG produce change regularly. As such there is a need to manage properly documents update everything from CIC WG membership lists to the latest CAB Record of Decision to an up to version of the FMN JMEI templates.



Travel: Due to the meeting schedule of the FMN initiative and its working groups, there is considerable Travel associated with this service.

Service Request: The service can only be requested as follows:

- ACO funded: via the CSLA (SLIN13.1 and Activity 525);

Service Flavours: The service comes as a complete package and is originally based on the scope of ACO funded tasks and funding levels described in 6300/TSC-FCX-0010/TT-140441/Ser:NU1023 dated 7 NOV 14. Over the intervening years this has evolved to keep pace with demand and those tasks pertaining to NATO Command Structure as an Affiliate to FMN Framework (NCSaaA) have been split out from FMN001 into FMN002.

Available on: The SME provide the following types of service to ACO through the following networks:

- Support to FMN Management and working group structures that support the direction and development of the FMN Framework: Unclassified (DNBL FMN Secretariat Portal)/NR (Advice)/NS (Advice)
- Support to derisking of the implementation of federated capabilities through collective and federated CIAV testing with other Affiliate Nations: Unclassified (DNBL CIAV Portal)/NR (Advice)/NS (Advice)/CV2E (federated CIAV laboratory).

Service prerequisites: N/A

Underlying Services: PLT001

Standard Service Support Levels: N/A

Available/Related NCI Academy Training not covered by service cost:

A0104	NATO CIS Planning

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. The service charge should take into account the extensive TDY commitment.

FMN002 Support NCS as an Affiliate to Federated Mission Networking (FMN)

Service ID: FMN002

Service Name: Provision of Support to the NATO Command Structure (NCS) as an Affiliate (NCSaaA) to the Federated Mission Networking (FMN) Initiative.

Portfolio Group: Other

Service Description: The scope of this service is to support Allied Command Operations (ACO) in order for the NATO Command Structure (NCS) to contribute as an Affiliate and conduct activities to maintain the Federated Mission Networking (FMN) Framework.

Value Proposition: With NAC approval of NFIP Vol 1 on 29 January 2015 (C-M(2015)0003-AS1), the NCS itself is committed to participate as an Affiliate to the FMN Initiative and therefore need to contribute to the maintenance of the FMN Framework (the roles of the NATO entities to enable the NCS to participate within FMN is described in MC0660, dated 15 January 2018). This service is to maintain ACO's portion of the NATO funded support to enable the NCSaaA to take part in the FMN framework. The maintenance of ACT's portion of the NATO funded support to enable the NCSaaA to take part in the FMN framework is funded via the ACT POW.

Service Features: The Service provides the following areas of expertise and facilities:

- **Support the Management of the NCSaaA**
 - a. Provide support to ACOS J6 within his role as NCSaaA Representative within the FMN Management Group (MG) in accordance with the NAC approved MC 0660 (Final) - Military Committee Directive to the NATO Command Structure for Participation as an Affiliate Within Federated Mission Networking¹, dated 15 January 2018 in order to;
 - (1) Provide support and inputs for NCSaaA participation in FMN MG Meetings - contribution to preparation, Lines to Take;
 - (2) Provide comments to Information Briefs, Decision Briefs, agenda, content, and record production.
 - b. Provision of technical advice in support of NCSaaA routine preparation for Military Committee Working Group (CIS format) meetings prior and after the FMN MG and FMN MG Preparation meetings;
 - c. Provide support to NCSaaA tasks by giving timely and relevant contribution to the documents, presentations, briefings, dashboards, reports for all key events and meetings with NCSaaA participation;

¹ The NCSaaA (MC0660) is composed of Allied Command Operations (ACO), Allied Command Transformation (ACT) and the NCI Agency (as the Communication and Information System (CIS) Service Delivery partner to NATO and as Service Management Authority (SMA) for NATO-led Mission Networks).

- **Support the Representation of NCSaaA within the FMN Operational Coordination (OC) Working Group (WG)**
 - a. Provision of operational analyses to support the collection, prioritization and consolidation of NCSaaA Interoperability Operational Requirements (IORs) for inclusion within the FMN Operational Requirements process;
 - b. Provide operational analysis in support to operational NCSaaA Subject Matter Experts (SMEs) across communities of interests that are participating in the FMN Inter-Working Groups (IWG) Syndicates¹ to develop Information Exchange Requirements (IERs) and Procedural Instructions (PIs);
 - c. Support the identification and management of the IERs, functional and non-functional requirements and engage and maintain communication with FMN stakeholders;
 - d. Analyse and provide relevant inputs to the FMN Spiral Specification Roadmap, particularly the linkage between IORs and Capability Enhancements (CPEs);
- **Provide representation of NCSaaA within the FMN Change and Implementation Coordination (CIC) WG**
 - a. Represent NCSaaA as the Affiliate lead within FMN CIC WG;
 - b. Management of NCSaaA Requests for Change (RFC) to the FMN Product Baseline;
 - c. Monitor and report progress of operational and technical advancement of NCSaaA against FMN Spiral Specifications, provide inputs to FMN Service Catalogue; FMN Fielded Baseline; FMN Forward Schedule of Change (FSC);
 - d. Manage NCSaaA integration of RFCs to the FMN Baseline;
 - e. Lead impact assessments for NCSaaA of FSC announced changes to the collective FMN Fielded Baseline;
 - f. Support the development of coherent FMN Service Management processes, systems and organizations across NCSaaA in accordance with NCIA role as Service Management Authority (SMA) for NATO-led Mission Networks;
 - g. Support execution and contribute to the annual technical assessment of federation at the exercises (e.g. STCO) and provide actionable insights and recommendations based on the analysis of lessons learned;
 - h. Support and contribute to the development of NCSaaA Individual Goals and NCSaaA Spiral Implementation Plan.

¹ Each IWG Syndicate operates across three Spirals, delivering at different stages key Federated and Interoperable Operational requests

- i. Provide support to NCSaaA FMN gap analysis and recommendations on addressing FMN-related interoperability gaps towards the FMN Spiral specifications in operational use.
- **Provide representation of NCSaaA within the FMN Coalition Interoperability, Assurance and Validation (CIAV):**
 - a. Provide the NCSaaA as the Affiliate lead within FMN CIAV WG
 - b. Support and contribute to the definition of the NCSaaA Individual Goals and Spiral Implementation Plan
- **Perform technical de-risking within CWIX technical focus areas and the CWIX FMN Exercise and provide actionable insights and recommendations based on the analysis of lessons learned.**

Travel. Due to the meeting schedule of the FMN initiative and its working groups, there is considerable Travel associated with this service.

Service Request: The service can only be requested as follows:

- ACO funded: via the CSLA (SLIN13.1 and Activity 525);

Service Flavours: The service comes as a complete package and is originally based on the scope of ACO funded tasks and funding levels described in 6300/TSC-FCX-0010/TT-140441/Ser:NU1023 dated 7 NOV 14. Over the intervening years this has evolved to keep pace with demand and NCSaaA tasks have been split out from FMN001 into FMN002.

Available on: The SME can provide services/advice through the following networks:

- Support to ACO, ACT and NDS that support the direction and development of the FMN Framework for the NCSaaA: Unclassified (MS Teams)/NR (Advice via Reach)/NS (NS DNBL VeVA MN Gov & Mgt Portal)
- Support to derisking of the implementation of federated capabilities through collective and federated CIAV testing with other Affiliate Nations: Unclassified (DNBL CIAV Portal)/NR (Advice)/NS (Advice)/CV2E (federated CIAV laboratory).

Service prerequisites: N/A

Standard Service Support Levels: N/A

Available/Related NCI Academy Training not covered by service cost:

A0104	NATO CIS Planning

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. The service charge should take into account the extensive TDY commitment.

FDM001 Federated Network Design and Service Management - Vigilance and Enhanced Vigilance Mission Network (VeVA MN)

Service Name: Federated Network Design and Service Management - Vigilance and Enhanced Vigilance Mission Network.

Service Type: Customer Facing.

Portfolio Group: Other Service.

Service Status: Available.

Service Description: As the federation Service Management Authority (SMA) for the VeVA Mission Network (MN), the NCI Agency has a critical role in supporting Supreme Allied Commander Europe (SACEUR) in the exercising of Command and Control (C2) over the forces assigned by Nations for the execution of the Family of Plans (FoP) for the Defence and Deterrence of the Euro-Atlantic Area (DDA) and the Allied Reaction Force (ARF) (when acting as SACEUR's strategic reserve). This service supports the design and management of the federation of services between NATO networks and the networks of the Nations that are committed to provide forces to the DDA FoP. As part of this service, NCI Agency as federation level SMA prepares and maintains the essential design documents, oversees federation activities, manages change and maintains configuration between the Mission Network Participants (MNP), as stipulated in the ACO Directive for the of the VeVA Mission Network (ACO Directive 080-125). In its capacity as SMA for the federation, NCI Agency uses this service to perform its formal roles in the Governance and Management structure stipulated in the directive. This service only covers the federated aspects of Governance and Management, federated service design and federated service transition. It does not cover the federated aspects of service operations. Federated Service Operations should be the subject of a separate service, noting split of respective responsibilities of NCI Agency and NCISG.

Value Proposition: Council approval of NATO FMN Implementation Plan Vol 1 on 29 January 2015 (C-M(2015)0003-AS1), established that each Mission Network established would require a single SMA, so that each mission network would operate under a single, centralized management model. In line with its existing technical authority role under SACEUR/GM NCIA C2 arrangements (SH/CCD J6/PT A/27 4/15-31 0233), NCI Agency is also appointed as the SMA for MN federations supporting NATO-led operations or missions (MC0660). NCI Agency has created a service that enables it to act as federation level SMA for ACO and to provide support to a federation that has been established between NATO Networks and the Networks of the Nations in line with the FMN Framework and which is governed and managed in line with FMN templates.

Service Features:

NCI Agency support as SMA to VeVA MN Governance and Management is comprised of the following packages that are scaled as follows:

- Support Routine VeVA MN Governance and Management. This is a foundation package providing year round support for VeVA MN Governance and Management and routine change management.
 - Scope parameters:
 - The driver for the preparation of products to support the SMA inclusion in routine governance and management is driven by the routine standing battle rhythm of for the VeVA Mission Network. This is stipulated in ACO Directive 080-125;
 - Routine change management managed around the monthly meetings of the VeVA MN Change Advisory Board (CAB) and held every month, except when a Steadfast Cobalt event is in execution. The scale of each routine change event is anticipated to be no more than:
 - Max Participants: 10 HQs/Units;
 - Planning conferences: One planning conference;
 - Services in scope : Up to 10 Services;
 - Execution timeline: 1 week.
 - Products typically provided or supported via this package:
 - Representation of NCI Agency in its capacity as SMA for the federation:
 - Represent WGs and Boards at Steering Group (SG) where NCIA is in lead;
 - Represent WGs and Boards at Executive Group (EG) where NCIA is in lead;
 - Represent SMA at SG;
 - Represent SMA at EG;
 - Represent SMA at Change Advisory Board (CAB);
 - Represent SMA at Security Accreditation Board (SAB);
 - Represent SMA at Operational Requirements Working Group (ORWG)/Operational Requirements Board (ORB);
 - Represent CAB at ORWG/ORB;
 - Represent SAB at CAB;
 - Represent CAB at SAB.
 - Minutes:
 - Produce CAB minutes;
 - Contribute to EG and SG minutes;
 - Contribute to SAB minutes.
 - Management Products:
 - Working Group Resourcing Annual Report;
 - Contributions to Strategic Roadmap (SRM) and SRM Action Plan;
 - Contributions to Gap list for Operational CIS WGs of the ARF and Joint Task Force HQs;
 - Contributions to Federation and Confederation Operational Requirements List;
 - Contributions to Federation and Confederation Information Exchange Requirements (IERs);

- Federation and Confederation Service Strategy and Service Roadmaps;
- Federation and Confederation Service Architecture;
- Federation and Confederation Joining Membership and Exit Instructions (JMEI) Vol IV;
- Federation and Confederation JMEI Vol I, II, III;
- Federation and Confederation Service Management and Control (SMC) processes and SoPs;
- Federation and Confederation MN Baseline;
- Federated Forward Schedule of Change;
- Community Security Requirements Statement (CSRS);
- Oversight and assessment of Federation and Confederation Statements of Compliance;
- Federation and Confederation Security Architecture and Accreditation Processes;
- RFC Impact Analysis Report for CAB;
- Contributions to Planning Products for Strategic CIS Planning Group (SCPG);
- Planning Products for Change Events.
- Activities:
 - Tracking of Requests for Change (RFC) to MN Baseline for CAB;
 - Service Replanning to implement RFC;
 - RFC assessment by CAB;
 - RFC Closure;
 - Federation and Confederation Digital Certificate Management;
 - Federation and Confederation Security Accreditation;
 - Management of Federation and Confederation Configuration Items in IO Core;
 - Federation and Confederation Firewall Change Management coordination;
 - At Change Event, SMA Oversight of Federated and Confederated Services;
- Facilities provided as part of this package:
 - Portal for Gov & Mgt Info Mgt [via supporting service PLT001].
- The service description and costing is valid for the event parameters as described above. Any change in those parameters must be complemented by a relevant Customer Request Form specifying the scope and associated funding, subject to a dedicated project covering requested activities.
- Support VeVA MN Major Change Events. These are events that support a Joining/Exiting Event for units and headquarters supported by the VeVA MN that have defined C2 roles in the DDA FoP.
 - Scope parameters: It is anticipated that these are executed quarterly, except when Steadfast Cobalt event is in execution (i.e. 3x per year). The scale of each major change event is anticipated to be no more than:

- Max Participants: 15 HQs/Units;
- Planning conferences/duration: One planning conference;
- Services in scope : Up to 35 Services;
- Execution timeline: 2 weeks.
- Products typically provided or supported via this package (requiring additional effort above the foundation package):
 - Representation of NCI Agency in its capacity as SMA for the federation:
 - Represent SMA at CAB;
 - Represent SAB at CAB;
 - Represent SMA at SAB;
 - Represent CAB at SAB.
 - Minutes:
 - Produce CAB minutes;
 - Contribute to SAB minutes.
 - Management Products:
 - Updates to Federation and Confederation Service Architecture;
 - Updates to Federation and Confederation JMEI Vol IV;
 - Updates to Federation and Confederation JMEI Vol I, II, III;
 - Updates to Federation and Confederation SMC processes and SoPs;
 - Updates to Federation and Confederation MN Baseline;
 - Updates to Federated Forward Schedule of Change;
 - Updates to Federation and Confederation Security Architecture;
 - Federated Planning Products for Change Events;
 - Contributions to Event Reports;
 - Activities:
 - Tracking of Requests for Change (RFC) to MN Baseline for CAB;
 - RFC assessment by CAB;
 - RFC Closure;
 - Federation and Confederation Security Accreditation;
 - Management of Federation and Confederation Configuration Items in IO Core;
 - Federation and Confederation Firewall Change Management coordination;
 - At Change Event, SMA Oversight of Federated and Confederated Services;
- The service description and costing is valid for the event parameters as described above. Any change in those parameters must be complemented by a relevant Customer Request Form specifying the scope and associated funding, subject to a dedicated project covering requested activities.
- Support an annual Exercise STEADFAST COBALT (STCO). This is a package that supports the federated Design and Management aspects of the annual Ex STCO event held to enable the headquarters and units of each new rotation of the Allied Reaction

Force (ARF) and potentially other Regional Plans Units and headquarters to join the VeVA MN.

- Scope parameters: Ex STCO is executed annually, scheduled in the year to enable the ARF to be prepared for its certification exercises. The scale of Ex STCO is anticipated to be no more than:
 - Max Participants: 50 HQs/Units;
 - Planning conferences/duration: Four planning conferences with additional meetings for SMA coordination, IER workshop, Academics and Exercise Specification meetings;
 - Services in scope : Up to 35 Services;
 - Execution timeline: up to 3 weeks for PhIIIA (federation Joining V&V), 4 weeks for PhIIIB (federation V&V).
- Products typically provided or supported via this package (requiring additional effort above the foundation package):
 - Representation of NCI Agency in its capacity as SMA for the federation:
 - Represent SMA at CAB;
 - Represent SAB at CAB;
 - Represent SMA at SAB;
 - Represent CAB at SAB;
 - Minutes:
 - Produce CAB minutes;
 - Contribute to SAB minutes;
 - Management Products
 - Updates to Federation and Confederation Service Architecture;
 - Updates to Federation and Confederation JMEI Vol IV;
 - Updates to Federation and Confederation JMEI Vol I, II, III;
 - Updates to Federation and Confederation SMC processes and SoPs;
 - Updates to Federation and Confederation MN Baseline;
 - Updates to Federated Forward Schedule of Change;
 - Updates to Federation and Confederation Security Architecture;
 - Contributions to Exercise Specification (EXSPEC);
 - Federated Planning Products for STCO;
 - Introductory Material and Questionnaires;
 - Contributions to Event Reports.
 - Activities:
 - Tracking of Requests for Change (RFC) to MN Baseline for CAB;
 - RFC assessment by CAB;
 - RFC Closure;
 - Federation and Confederation Security Accreditation;
 - Management of Federation and Confederation Configuration Items in IO Core;
 - Federation and Confederation Firewall Change Management coordination;

- At Ex STCO, SMA Oversight of Federated and Confederated Services.
- The service description and costing is valid for the event parameters as described above. Any change in those parameters must be complemented by a relevant Customer Request Form specifying the scope and associated funding, subject to a dedicated project covering requested activities.

Service Ordering and Request: The service can only be requested as follows:

- Sponsor: SHAPE Cyberspace J6 SPP
- ACO funded: via the CSLA (SLINxx) [TBC];
- Notes:
 - Sponsor needs to confirm to NCI Agency the number of major change events expected in the upcoming year and the scope of Ex STCO. This will scope the size of Packages 2 and 3. The default is 3x major events. Note that in 2025, Ex STCO25A and STCO25B were held, equating to one STCO event and one major change event.;
 - It is assumed that at steady state of the VeVA MN there will only be one Ex STCO per year (in the Autumn) and that STCO will in future only focus on the upcoming ARF rotation.
 - It is assumed that NCISG will continue to provide the VeVA Core MN SEWG Sub-WG chair roles in STCO and Major Events [TBC when ACO Directive 080-125 is signed].

Service Flavours: If other federations between NATO Networks and the Networks of the Nations need to be supported with a federation level SMA in line with the FMN Framework, then the above service packages can be replicated and scaled appropriately and created for the services federated in line with the same pattern (FDM00x):

- **Large Network federation**, of a similar scale to VeVA MN. An example of this would be the the governance and management of the NS federation that has been established as Allied Federated Services (AFS);
- **Small Network federation**, of a similar scale to the former NATO Responcs Force (NRF) Mission Network or the creation of an out of area Mission Network for the Allied Reaction Force.

Available on: The SMA can provide services/advice through the following networks:

- NATO SECRET;
- NATO SECRET Releasable to VeVA.

Service Prerequisites: This service relies upon:

- PLT001 – for the provision of the Portal for the Info Mgt for the Gov & Mgt structures.

Standard Service Support Levels: N/A.

Service Reporting / KPI:

Foundation package	Deliverables	KPIs

Management	1.1. Quarterly Report to VeVA Governance and management structure on SMA activities.	Report to the VeVA Governance and Management structure by reporting by 01 April, 01 July, 01 Oct, and 31 Dec each year.
Contributions	1.2. Active contributions to VeVA MN Governance and Management	- Representation of NCI Agency in its capacity as SMA for the federation (see above) - Maintenance of Governance and Management Products (shared responsibility) (see above) - Maintenance of Management Products (SMA responsibility) (see above) - Throughput of routine RFC to VeVA Baseline - Success of RFC Packaging into Event - Minimised Operational Disruption
Major Change Events	Deliverables	KPIs
Contributions	1.3. Encompassed by SMA contribution to the Event report.	- Production of Event Report. - Throughput of major change RFC to VeVA Baseline - Success of RFC Packaging into Event - Minimised Operational Disruption
STCO	Deliverables	KPIs
Contributions	1.4. Encompassed by SMA contribution to the Ex STCO Interoperability report and Exercise report.	Interoperability report and Exercise reporting structure and timings (see EXSPEC).

Available NCI Academy Training not covered by service cost:

A0104	NATO CIS Planning

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. The service charge should take into account the TDY commitment.

Annex C – Other Standard Products

INF046 Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service

Service ID: INF046

Service Name: Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service

Portfolio Group: Infrastructure Services

Service Description: NRA IPv6 LIR service looks forward to IPv6 with an aim to enable nations to have their own block of address space. The NCI Agency Naming and Registration Authority (NRA) is a registered LIR (Local Internet Registry) thus able to sponsor and 'resell' IP address space, the INF046-D service flavour provides a cost centre addressable to the Nations for procurement and ongoing administration of IPv6 addresses. In this service offering the NRA will procure, administer and protect the address allocation with the relevant Regional Internet Registry, the requirement for management of the address space within the nation network remains with the nation, where NRA will offer consultation via INF046-C.

Value proposition: This service provides value to customers through the collation and sharing of centrally registered items Alliance-wide, improving data integration, assuring global uniqueness, and protection from collisions in names, numbers and semantics. As organizations become data-enabled, simultaneous with an accelerating data velocity, the criticality of master data management has grown to be an imperative. IPv4 address has all but run out, few nations are fortunate enough to already possess their own block of IP address. For the Service flavour, IP Sponsoring LIR (Local Internet Registry) NRA will act as a Sponsoring LIR for a NATO nation wishing to procure IPv6 address space for national, NATO secret, mission or AFS use. Further NRA will consult and advise on best application of this new technology within the Nation or entity.

Service Features: This service offering provides Nations and NATO affiliated entities the capability to procure their own IPv6 address space through NATO. This will in the future be a key enabler on both the NU (Internet) and MS/NS networks under both FMN and AFS. Further providing consultancy service to support the deployment and roll out of IPv6 technology.

Service Flavours: NRA offers different flavours according to different data spheres

INF046-C IPv6 Consultation: Consultation enables advice and registration on the usage, deployment and transition to IPv6. One time consultation is a prerequisite for INF046-D. Included in this cost is the consultation on super-net addressing plan following AFS principals (nation manages addressing). Further Consultation may be purchased provided per Subnet Allocation.

INF046-D IPv6 Sponsoring LIR NRA: Sponsorship enables a nation (or entity) to receive a single allocation of IPv6 address space. This is an annual reoccurring service for maintenance and sponsorship of IPv6 address space, instantiation of this flavour requires consultation (INF046-C) for the super-net allocation.

Available on:

All Networks

Service Prerequisites: NATO member, NS nation connection is behind a NNG (AFS) or for a none-NATO nation, the MS connection is behind a NIP (FMN)]

Standard Service Support Levels:

Service Availability¹ Target: *[During heavy load times BAU requests will receive lower priority than mission critical warfighting requests. Registration and allocation services work on a 2 week (10 working day) delivery window, however this may be further delayed if provided information is not thorough and correct. This delivery window is to facilitate clarifications, ensuring forward planning and data integrity; once registration and allocation are complete, a new ticket must be raised for changes and amendments not in the original ticket.]*

Service Restoration: *[For service degradation NRA will act (MTTR) within 1 working day of an incident notification, NB in some instances full restoration will be beholden to the vendor timelines and availability.]*

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.]

Service Cost / Price: INF046-C flavour is costed per allocation per Security domain. INF046-D is costed per allocation (recommended each nation 1x allocation). Ongoing annual service will cover administration, de-confliction, cessation, maintenance, monitoring and reporting.

¹ The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

*Minutes available during agreed reporting period excluding planned maintenance minutes