Duty Location: Northwood, UK

JOB DESCRIPTION
Head – CIS Security
Directorate of Service Operations – CSU Northwood
Grade: G15

This is a position within the NATO Communications and Information Agency (NCI Agency), an organization of the North Atlantic Treaty Organization (NATO).
The NCI Agency has been established with a view to meeting to the best advantage the collective requirements of some or all NATO nations in the fields of capability delivery and service provision related to Consultation, Command & Control as well as Communications, Information and Cyber Defence functions, thereby also facilitating the integration of Intelligence, Surveillance, Reconnaissance, Target Acquisition functions and their associated information exchange.
The Director of Service Operation (DSO) is accountable to plan, install, operate and maintain Computer Information Systems (CIS) services throughout the allocated Area of Responsibility (AOR), in static NATO Headquarters, Alliance Operations and Missions and Exercises, and supported Organisations. Service Operations are delivered and managed in close coordination with the Directorates of Applications Services, Infrastructure Services, AirC2 Services and BMD Services. DSO and the CSUs receive support from the Agency's Enabler functions (General Services, Human Resources, Finance, and Acquisition). DSO is the signature authority for Agency orders involving deployment of staff and equipment to operations and exercises and is responsible for maintaining operational situational awareness of and reporting on all Agency Communication and Information System (CIS) operations and services. DSO directs Asset Management and logistic support of all the NATO owned CIS equipment. The Service Operations organisation comprises the following organisational entities: The Integrated Operations Centre (Ops Centre) provides continuous monitoring, response, control and reporting capabilities for the NCI Agency's CIS infrastructure and services; The Operation and Exercise SL supplies C2 Catalogue Services to customers that are planning and/or executing deployed operations and exercises and for the implementation of the C2 arrangements between SACEUR and the General Manager of NCI Agency; The CSSC provides Engineering, Logistical, technical advice to NCI Agency service lines and customers and operational support services to include deployable CIS logistics sustainment capabilities in support of operations and exercises; and, The CSUs deliver the installation, operation, maintenance, protection, cyber security and support of CIS systems to provide services within the AOR and as defined in SLAs and other agreements.
NCI Agency CIS Support Unit (CSU), located in Northwood (UK) together with the CIS Support Element in Yeovilton, and RAC Molesworth, enables end-to-end CIS services as it installs, operates, maintains and supports the full range of CIS capabilities during peacetime, crisis and war throughout its allocated Area of Responsibility (AOR) and as otherwise directed.

Duties:

Under the direction of Commander CSU Northwood, NSO OOX 0010, the incumbent will perform duties such as the following:

- Acts as the primary CIS Security expert and provides advice to the CSU Commander on all CIS Security (Communications Security and Computer Security) matters. Directs the activities of the COMSEC technicians, ensuring the COMSEC and Crypto Custodian programs strictly adhere to higher Headquarters policies, to include COMSEC pre-inspections;
- Produces and updates security accreditation documents for CSU Northwood-managed systems within the CSU Northwood Area of Responsibility (AOR). Coordinates with the Security Accreditation Authority, through the Accreditation Support Office to maintain security accreditation;
- Supports all phases of the security accreditation processes required to maintain operational status including conducting Security Testing and Validation Plans (STVPs);
- Monitors the Cyber security status of all CSU Northwood managed systems, and identifies security-related Key Performance Indicators (KPIs) and generates reports to ensure full visibility of the overall CSU's Information Security posture;

- Coordinates and oversees penetration testing and vulnerability assessments by the NATO Cyber Security Centre (NCSC), Systems Security and Evaluation Agency (SECAN), or other bodies performed on CSU Northwood's networks or elsewhere as directed;
- Assists with complex remediation activities as directed internally or by NCSC including incident handling;
- Assess all change requests, access requests, and interconnection requests from a CIS security perspective;
- Provides feedback, advice and guidance to senior management in areas of enterprise architecture, NATO security accreditation activities, procurement as well as training and awareness programmes;
- Provide assistance to security investigations by MARCOM HQ, Alied Comand Counter Intelligence (ACCI), and various other (external) stakholders; when related to CSU AOR (provided) services;
- Reports security incidents to MARCOM (HQ security office), and NCSC;
- Reports significant risks and compliance issues to MARCOM HQ;
- Responsible for providing input to the annual O+M budget proposals;
- Represents the CSU in NATO Committees, Steering Groups/Boards, Technical Coordination Conferences and other events as required;
- Liaises with other NCI Agency entities and customers as required with authority to commit CSU resources as directed;
- Acts as the Divisional Security Officer for CSU Northwood;
- Deputize for higher grade staff, if required;
- Perform other duties as may be required.

Experience and Education:

- A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline (such as, working in a large organisation in a CIS Security Role) and 2 years post-related experience;
- Or exceptionally, the lack of a university degree may be compensated by the demonstration of a candidate's particular abilities or experience that is/are of interest to the Agency, that is, at least 6 years extensive and progressive expertise in duties related to the function of the post (such as, system security, security architecture, network security engineering, security governance, risk management, performance management and value delivery);
- Knowledge and experience using common security tools such as Tenable Nessus, Nmap, McAfee ePO, etc;
- Knowledge of common MS and Linux updating and patching systems, IT security frameworks and governance models, and Common Vulnerability Scoring System (CVSS) v2.0 and v3.X standards.

Desirable Experience and Education:

- ISC2 CISSP,ISC2 CCSP certification or ISCA CISM and OSCP certification;
- ISO/IEC 27001 Lead Auditor certification;
- Knowledge and working experience of security and network technologies such as IPv6; Firewalls, Virtual Private Networks, Public Key Infrastructure, Intrusion Detection and Forensic Appliances;
- Experience:
  - With dealing with security incidents, interpretation of CIS security auditing tool results;
  - With Wireless LAN technologies and Endpoint Security of mobile devices such as Laptops, Apple iOS devices (tablets and smartphones);
  - In conducting risk assessments;
  - In the provision or delivery of training;
  - Delivering presentations and briefings to large audiences.
- Knowledge and working experience of Microsoft Windows Operating Systems (Server 2012/2016 Windows7/Windows10);
- Knowledge of NATO Security Policy and supporting directives;
- Understanding of Cyberspace security challenges within NATO or a NATO member nation environment;
- Prior experience of working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organization, including ACO and ACT.

Language Proficiency:

- A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other is desirable.
- **NOTE:** Most of the work of the NCI Agency is conducted in the English language.

Competencies or Personal Attributes:

- Deciding and Initiating Action - Takes responsibility for actions, projects and people; takes initiative and works under own direction; initiates and generates activity and introduces changes into work processes; makes quick, clear decisions which may include tough choices or considered risks.
- Formulating Strategies and Concepts - Works strategically to realise organisational goals; sets and develops strategies; identifies, develops positive and compelling visions of the organisation's future potential; takes account of a wide range of issues across, and related to, the organisation.
- Relating and Networking - Easily establishes good relationships with customers and staff; relates well to people at all levels; builds wide and effective networks of contacts; uses humour appropriately to bring warmth to relationships with others.
- Delivering Results and Meeting Customer Expectations - Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals.

Travel:

- Business travel to NATO and national (NATO and non-NATO) facilities as well as frequent travel between the NCI Agency offices.
- May be required to undertake duty travel to operational theatres inside and outside NATO boundaries.

Professional Contacts:

The incumbent is responsible for:

- Maintaining liaison, as required, with related roles within NCI Agency, MARCOM HQ management staff, contractors, related organisations and industry partners in relation to CIS Security.

Supervisory/Guidance Duties:

- The incumbent may give professional guidance to staff.
- The incumbent may be required to perform briefs to staff and provide training.
- The incumbent will be required to develop and coordinate personal (staff) development plans as part of Performance Management. This should include training to develop a high level of technical knowledge of assigned equipment, ensuring quality of service and continuity of technical skills.

Working Environment: Normal office environment.

Security Clearance Level: NATO Cosmic Top Secret