



## JOB DESCRIPTION

### Post Details:

Post Title:	<b>Principal Technician (Cyber Security)</b>	Organisational Element:	CSU Northwood
Military/Civilian:	CIV	Location:	Northwood, UK

### Organization context:

This is a position within the NATO Communications and Information Agency (NCIA), an organization of the North Atlantic Treaty Organization (NATO).

To strengthen the Alliance through connecting its forces, the NCIA delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

### Organizational Element Statement of Functions:

Communications and Information Systems (CIS) Support Unit Northwood (CSU NW) installs, operates, maintains, defends, and supports CIS services and capabilities required by NATO Allied Maritime Command (MARCOM) during peacetime, crisis, and war. This role includes the delivery of critical CIS services to the NATO Standing Naval Forces in support of maritime operations and exercises. CSU NW operates and maintains the main NATO Communications Centre (COMMCEN), which provides NATO-wide formal messaging, ship broadcast, and submarine CIS services. CSU NW also provides oversight and assistance to the NCIA detachment in Yeovilton, UK, who provide CIS services for the NATO Joint Electronic Warfare Core Staff (JEWCS).

Service Operations Branch (SOB) provides local CIS support for all Agency services provided to MARCOM. SOB operates a 24/7 watch floor which delivers direct support to MARCOM Theatre Maritime Operations Centre (TMOC). This Branch is responsible for implementing local projects and changes, troubleshooting and maintaining services, applications, networks, and systems, and delivering CIS services to MARCOM ships on behalf of CSU NW.

### Job role description:

The Principal Technician (Cyber Security) assists with ensuring the ongoing confidentiality, integrity and availability of Agency systems and services. This is achieved through close collaboration with the NATO Cyber Security Centre and local security staff, with a focus on cyber security awareness and compliance, accreditation support and cyber incident response. They provide local subject matter expertise within the Cyber Security Domain. They monitor local compliance with Agency security policies and contribute to their

development, investigate cyber security incidents and educate employees on cyber security best practices and regulations.

## **Duties and Responsibilities:**

### **Information security**

- Applies and maintains specific security controls as required by organisational policy and local risk assessments.
- Communicates security risks and issues to business managers and others.
- Performs basic risk assessments for small information systems.
- Conducts security inspection and configuration activities of electronic devices.
- Contributes to the identification of risks that arise from potential technical solution architectures.
- Suggests alternate solutions or countermeasures to mitigate risks.
- Defines secure systems configurations in compliance with intended architectures.
- Supports investigation of suspected attacks and security breaches.

### **Information assurance**

- Follows standard approaches for the technical assessment of information systems against information assurance policies and business objectives.
- Makes routine recommendations for system accreditation decisions.
- Recognises decisions that are beyond their scope and responsibility level and escalates according.
- Reviews and performs risk assessments and risk treatment plans.
- Identifies typical risk indicators and explains prevention measures.
- Maintains integrity of records to support and justify decisions.

### **Specialist advice**

- Provides detailed and specific advice regarding the application of their specialism to the organisation's planning and operations.
- Actively maintains knowledge in one or more identifiable specialisms.
- Recognises and identifies the boundaries of their own specialist knowledge.
- Where appropriate, collaborates with other specialists to ensure advice given is appropriate to the organisation's needs.

### **IT infrastructure**

- Provisions/installs, configures and maintains infrastructure services and components.
- Monitors, measures and reports on infrastructure load, performance and security events.
- Identifies operational issues and contributes to their resolution.
- Carries out agreed operational procedures, including backup/restore, using supplied infrastructure tools and scripts.
- Carries out agreed system software maintenance tasks.
- Automates routine system administration tasks to specifications using standard tools and basic scripting.

### **Vulnerability Assessment**

- Undertakes low-complexity routine vulnerability assessments using automated and semi-automated tools.
- Escalates issues where appropriate.
- Contributes to documenting the scope and evaluating the results of vulnerability assessments.

#### **Information Security Administration**

- Works with access controls for firewalls and routers.
- Assists in the operation of day-to-day administrative transactions and systems.
- Performs periodic system backups and produces standard monitoring reports.
- Coordinates user access and maintains security checklists and authorization tables.
- Tests the effectiveness of new or revised information security procedures and tools.

#### **Information Technology (IT) Security Policies**

- Performs information gathering and research on key elements of IT security policies.
- Assists senior colleagues in identifying and analysing critical issues in IT security policies.
- Executes IT security policies and standards within a specific region in organization.
- Conducts performance reviews on implementation of IT security policies.
- Generates status reports for senior management to ensure the implementation of IT security policies.

#### **Additional duties for this post:**

- Acts as the alternate CIS Security Officer.
- Acts as the alternate Crypto Custodian and Communications Security (COMSEC) Subject Matter Expert for unit and operational partners.
- Assists in managing the receipt, custody, transfer, safeguarding, accounting and destruction of crypto material charged to the unit COMSEC account.
- Assists with maintaining up-to-date records of operational partner COMSEC requirements and submission of reports pertaining to reportable crypto material.
- Contributes to Asset Configuration Patching and Vulnerability Management activities.
- Maintains database of all CIS under the CSU's Geographical Area of Responsibility (GAoR) to include CIS user accounts, assigned roles, and access permissions.
- Maintains registers of removable or classified electronic storage media and conducts spot checks to ensure the proper custody and the accuracy of classification markings.
- Conducts security inspection and configuration activities of electronic devices.
- Provides CIS security event analysis, interpretation, and Level 1 support to external Agency entities and Cyber Security Service Line entities as required.
- Executes the incident management process in accordance with the Information Technology (IT) Information Library Version 4 framework.
- Maintains thorough familiarity with and close adherence to NATO, Headquarters Allied Command Operations (ACO) and Agency directives and procedures for handling cryptographic material.
- Deputize for higher-grade staff, if required.
- Perform other duties as may be required.

**Education, Experience and Training (essential):****Education:**

Higher vocational training in a relevant discipline with 3 years cyber-related experience or alternatively a secondary educational qualification with 5 years cyber-related experience.

**Experience:**

At least 3 years' experience in the implementing, and managing the underlying technology, software and hardware components that ensure the smooth functioning of servers, storage systems, data centers, and cloud services.

Practical experience troubleshooting infrastructure related issues, perform regular maintenance.

Extensive experience with Microsoft Windows desktop operating systems;

Extensive experience with Microsoft Windows server operating systems including the following key components such as Active Directory, Group Policy, New Technology File System permissions, Dynamic Host Control Protocol;

Experience with key Information Technology concepts including shared storage, clustering and virtualization;

Familiarity with security and network technologies such as IPv6; Firewalls, Virtual Private Networks, Public Key Infrastructure, Intrusion Detection and Forensic Appliances;

Familiarity with International Organization for Standardization (ISO)/International Electro-technical Commission (IEC) 27001 framework.

Adequate communication and interpersonal skills.

Good analytical skills and solution-oriented attitude.

**Training/Certifications:**

Information Technology (IT) Information Library Version 4 Foundation

**Education, Experience and Training (desirable):****Education:****Experience:**

Experience dealing with security incidents, interpretation of CIS security auditing tool results;

Experience with Wireless LAN technologies and Endpoint Security of mobile devices such as Laptops, Apple iOS devices (tablets and smartphones);

Experience with VMWare virtual hosting infrastructure and applications;

Experience using Microsoft update and patch management systems, IT security frameworks and governance models, and Common Vulnerability Scoring System (CVSS) v3.X or later standards;

Experience using Unix-based operating systems (e.g., Redhat Linux and Kali Linux);

Knowledge and experience using Trellix ePO and associated components (i.e., Trellix Agent, Endpoint Security Platform, Threat Prevention, Advance Threat Protection, Data Loss Prevention, Application Control, etc.);

Experience in conducting risk assessments;

Experience in the provision or delivery of training;  
Experience in delivering presentations and briefings to large audiences;  
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.

**Training/Certifications:**

Industry-recognized CIS security-related certification (e.g., CompTIA Security+, ISC2 CISSP, ISC2 Certified Cloud Security Professional (CCSP), Information Systems Audit and Control Association Certified Information Security Manager, Offensive Security Certified Professional, etc.);  
Industry-recognized ISO/IEC 27001 certification (e.g., Lead Auditor);  
CIS security-related certification from NATO, national military or governmental body;

**Behavioral competencies:**

- *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.
- *Adapting and Responding to Change* - Adapts to changing circumstances; tolerates ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people or situations; shows an interest in new experiences.
- *Achieving Personal Work Goals and Objectives* - Accepts and tackles demanding goals with enthusiasm; works hard and puts in longer hours when it is necessary; seeks progression to roles of increased responsibility and influence; identifies own development needs and makes use of developmental or training opportunities.