

NOTIFICATION OF A VACANCY

Post/Vacancy Number:	CSA GIX 0010
Grade:	A-2
Title:	Head(INFOSEC)
Division/Office:	NCSA Squadron Ramstein
NATO Body:	Brunssum Sector ISPE
Location/Country:	Ramstein, Germany
Closing Date:	31 March 2010
Point of Contact:	CHRM
Notice to Move:	N/A

PART II - PE DETAILS

A. POST CONTEXT

NCSA ensures the cost effective provision of secure end to end information exchange and processing services for NATO Consultation, Command and Control.

NCSA Sectors resource & plan, install, operate, protect, maintain and support CIS capabilities.

NCSA Remote Squadrons install, operate, protect, maintain and support CIS capabilities within parameters defined by the parent Sector.

Command Branch provides staff support, manages assigned resources, and coordinates and supervises all staff activities

INFOSEC is responsible for actively managing approved INFOSEC policy. It provides support, management and advice on all aspects of INFOSEC. It provides Local CRYPTO custodian function and acts as Local Distribution Agency (LDA) if required.

Head (INFOSEC) ensures local compliance with the ACO/NCSA CIS Security policy from higher Headquarters, ensures systems and networks are protected from all forms of attack, and provides the local Crypto custodian.

B. REPORTS TO

Branch Head (Command Branch), CSA GXD 0010.

C. PRINCIPAL DUTIES

The incumbent's duties are:

1. Acting as the primary INFOSEC technical expert for the Squadron and providing advice to Squadron Commander on all INFOSEC matters.
2. Planning, organising and exercising staff supervision over all aspects of INFOSEC activities.
3. Identifying system vulnerabilities and threats, and engineering Cyber Defence solutions. Ensuring the application of necessary safeguards (both technical and administrative) to minimize those vulnerabilities and defend against potential attacks, in coordination with the Head (Service Support Branch).
4. Providing engineering support for the integration of computer security best practices. Performing detailed technical reviews of system documentation to ensure computer security integrity.
5. Directing the activities of Squadron COMSEC technician, ensuring the COMSEC and Crypto Custodian programs strictly adhere to higher Headquarters policies, to include COMSEC pre-inspections.
6. Developing and administering the site security program, including monitoring, and ensuring the implementation of NATO security policies and procedures, as the primary responsible on COMPUSEC issues.
7. Assisting Customer INFOSEC in developing, implementing and managing security awareness and training for site users.
8. Providing technical input, diagrams, and documentation for system accreditation by Customer INFOSEC.
9. Providing advice and assistance in identifying security requirements for the different automated systems.
10. Performing risk assessments and identifying potential security risks that may arise.
11. Supporting Parent Sector in security incidents investigations and briefing the Sector/Squadron Commanders on recommended actions.

12. Responsible for providing input and assisting in the engineering of the Squadron Disaster Recovery/Business Continuity Plans in accordance with NCSA HQs Cyber Defence policy.
13. Maintaining close liaison with NITC and other external agencies on all computer-related security issues and on Border Protection Devices, Mailguards and gateways.
14. Responsible for problem analysis and solution testing beyond the technical abilities of subordinate technicians.
15. Responsible for providing input to the annual O+M budget proposals.
16. Developing and coordinating training program for subordinates, ensuring the effectiveness of such program as well as ensuring that the training addresses the impact of new technology and future systems.
17. Maintaining a close liaison with the technicians and engineers in the Squadron, as well as technicians and engineers in other NCSA Squadrons, Sectors and NCSA HQs.
18. Staying abreast of technological developments relevant to the area of work.

Legal authority is held: None

Budget authority is held: None

Decision authority is held: None

Supervisory duties: None

There are first line reporting responsibilities for the following numbers of staff: 2 x OR-7

D. ADDITIONAL DUTIES

The employee may be required to perform a similar range of duties elsewhere within the organisation at the same grade without there being any change to the contract

The incumbent may be required to undertake operation deployments and/or TDY assignments both within and without NATO's boundaries.

The work is normally performed in a typical Office environment. Normal Working Conditions apply. The risk of injury is categorised as: No Risk

PART III – QUALIFICATIONS

A. ESSENTIAL QUALIFICATIONS

1. Professional/Experience

Primary: 913D Business/information systems strategy and planning - Information security

The management of, and provision of expert advice on, the selection, design, justification, implementation and operation of information security controls and management strategies to maintain the confidentiality, integrity, availability, accountability and relevant compliance of information systems.

Primary Skill Level: Enable: Conducts security risk assessments for defined business applications or IT installations in defined areas and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls (e.g. the key controls defined in BS7799).

Information Systems Engineering and Maintenance - General

Information Systems Engineering and Maintenance - INFOSEC Implementation - Computer Security

Experience in development and implementation of INFOSEC planning and policies. Experience in evaluation and accreditation of telecommunications and information systems. Experience in security requirements analysis.

Secondary: 913E Business/information systems strategy and planning - Information assurance

The protection of systems and information in storage, processing, or transit from unauthorised access or modification. Denial of service to unauthorised users; or the provision of service to authorised users. Includes those measures necessary to detect, document and counter threats to the integrity of stored information, such as the application of firewalls and intrusion detection systems (IDS).

Secondary Skill Level: Enable: Investigates suspected attacks and recommends remedial action. [Ref: SFIA v3 2005:INAS]

Knowledge and use of IT security tools and techniques in developing effective COMPUSEC

procedures.

Broad and in-depth knowledge of COMSEC and COMPUSEC principles, and their application to the development of effective INFOSEC programs.

2. Education/Training

University Degree and 2 years function related experience, or a Higher Secondary education and completed advanced vocational training leading to a professional qualification or professional accreditation with 4 years post related experience.

Courses:

NCISS-004 NATO Communications Security Cryptographic Custodian - NATO CIS School

NCISS-278 INFOSEC (COMSEC) - NATO CIS School

NCISS-279 INFOSEC (COMPUSEC) - NATO CIS School

M-5-32 NATO Staff Officer Orientation Course (NU Rel Pfp MD EU) - NATO School Oberammergau (DEU)

3. Security Clearance

COSMIC TOP SECRET/B

4. Language

English SLP 3333 (Listening, Speaking, Reading and Writing)

NOTE: The work both oral and written in this post and in this Headquarters as a whole is conducted mainly in English.

5. Standard Automatic Data Processing Knowledge

Word Processing:	Working Knowledge
Spreadsheet:	Working Knowledge
Graphics Presentation:	Working Knowledge
Database:	Working Knowledge
email Clients/Web Browsers	Working Knowledge
Web Content Management:	Basic Knowledge

B. DESIRABLE QUALIFICATIONS

1. Professional/Experience

Specialisations: Demonstrable evidence in maintaining knowledge of advances in IS engineering and Service Management.

Specific Experience: Specific experience in an INFOSEC post.

Experience is Risk Management.

Experience as a System Administrator in a Windows Environment

CISSP Certification

Security + Certification

Experience in NATO or NATO Nation Crypto policies and procedures

Experience with IT security analysis and evaluations

Experience with NATO or NATO Nation Emanation Security Policies

2. Education/Training

ITIL Foundation Certificate

Graduate diploma in an IS engineering related subject.

M4-30-P - NATO RMEP Course, M

3. Language

C. CIVILIAN POSTS

1. Personal Attributes

Uses independent judgement to propose solutions based on parent Sector guidance and NITC directives.

Possesses excellent computer security skills.

Possesses good inter-personal and communication skills, tact, judgement and adaptability combined with the strength of character to openly state system limitations and mandatory security requirements.

A sense of diplomacy and propriety in order to work harmoniously with colleagues and other staff, both civilian and military, from NATO and NATO nations.

2. Managerial Responsibilities

There are first line reporting responsibility for the following numbers of staff: 2 x OR-7

3. Professional Contacts

Interfaces with Parent Sector, High HQs staff, NITC staff, contractors, Customer Technical and INFOSEC staff.

4. Contribution to the Objectives

Ensures the Squadron's IT security posture conforms to Higher HQs INFOSEC policies and ensures Cyber Defence protection of Squadron's IT Systems and Customer's Data from threats.

5. Work Environment

The work is normally performed in a typical Office environment. Normal Working Conditions apply. The risk of injury is categorised as: No Risk.

D. Remarks