

	<p>NATO AEW&amp;C PROGRAMME MANAGEMENT AGENCY</p> <p><b>NOTIFICATION OF VACANCY</b></p>
<p>Post Title:</p>	<p>FLEP CIS Security Officer</p>
<p>Post Number:</p>	<p>PMA92</p>
<p>Duty Location:</p>	<p>Brunssum, The Netherlands</p>
<p>NATO Grade</p>	<p>A3 / NATO Grade 17</p>
<p>Nation:</p>	<p>NU</p>
<p>Division/Office</p>	<p>Programme Management Division</p>
<p>Branch/Section</p>	<p>Information Assurance IPT</p>
<p>Clearance:</p>	<p>NATO Secret (NS)</p>
<p>Manages/Supervises (no. of staff)</p>	<p>N/A</p>
<p>Closing Date</p>	<p>Friday, 6 January 2023</p>
<p>Point of Contact</p>	<p>Human Resources &amp; General Services Office <a href="mailto:recruitment@napma.nato.int">recruitment@napma.nato.int</a></p>
<p>Application Details:</p>	<p>A NAPMA Application Form of any applicant should be forwarded by email to <a href="mailto:recruitment@napma.nato.int">recruitment@napma.nato.int</a> The application form can be downloaded at <a href="http://www.napma.nato.int">www.napma.nato.int</a>.</p> <p>NAPMA can only employ nationals from the NAPMO nations for this position. Applications should be supported by the member of the Board of Directors of the respective nation.</p>

**1. POST SUMMARY:**

NAPMA is a NATO Agency responsible to plan, acquire, and deliver improvements to and support the sustainment of the NATO AEW&C capabilities, while ensuring technical airworthiness, following the guidance of the NAPMO Nations. The Final Lifetime Extension Programme (FLEP) Communication and Information Systems (CIS) Security Officer is responsible for providing oversight on the implementation of CIS security controls, measures and procedures across all FLEP environments in accordance with NATO security policies. As directed, this position will embed with NAEW&CF or Mission System Engineering Centre (MSEC) at Geilenkirchen Airbase to execute the full scope of designated duties.

## **NATO UNCLASSIFIED**

### **2. PRINCIPAL DUTIES**

Responsible to the Air Safety and Information Assurance Engineer (PSA01) for the following duties:

- Supporting all phases of the NATO security accreditation processes required to gain and maintain security accreditation and authorization to operate for the FLEP modified NE-3A Weapons System.
- Coordinating and overseeing risk assessments, security test & verification, security audits, vulnerability assessments and penetration tests; overseeing remediation activities and reporting on progress;
- Formulating, coordinating and maintaining security operations procedures (SecOps) for all FLEP CIS environments in coordination with all security stakeholders;
- Auditing the implementation and maintenance of hardware, firmware and software modifications and enhancements to the CIS to ensure that security is maintained and reporting to the CISOA, CISP and the SAA any detected CIS security weaknesses and vulnerabilities;
- Overseeing security monitoring and incident response programs; managing and investigating CIS security incidents in close coordination with the security organization, the CISOA, the CISP, the SAA and, when required, NATO incident response and counter-intelligence agencies.
- Maintaining a record of all persons authorized to use any part of the CIS and the extent of their authorization and ensuring that those persons have the security clearance and need-to-know for the information handled in the CIS;
- Ensuring the proper custody of computer storage media as well as carrying out spot checks and maintaining records of checks on the presence of classified computer storage media and on the accuracy of their markings;
- Utilizing security incident event management and security log analysis tools to identify security issues, develop assessments and present to security stakeholders.

### **3. SPECIAL REQUIREMENTS AND ADDITIONAL DUTIES:**

The incumbent may be required to perform other related duties as directed.

### **4. ESSENTIAL QUALIFICATIONS AND EXPERIENCE:**

A minimum requirement of a Bachelor's degree at a nationally recognized/certified University in an Information Security related discipline and 3 years post-related experience; or at least 6 years extensive and progressive expertise in duties related to the function of the post. Possession of one of the following industry certifications: Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP) or Certified Information System Manager (CISM); or possession of another industry information/cyber security certification. At least two years' experience with system security, security architecture, network security engineering, security governance, security audit or security risk management.

Must be fluent in one of the two NATO Official languages; some knowledge of the other is desirable. However, the work in NAPMA, both oral and written, is conducted in English.

**NATO UNCLASSIFIED**

## NATO UNCLASSIFIED

### 5. DESIRABLE QUALIFICATIONS AND EXPERIENCE

Advanced degree in computer science, information technology or a closely related technical field. Current knowledge and experience with NATO CIS Security accreditation and related NATO security policies and supporting directives. Knowledge and working experience with Security Incident Event Management (SIEM) processes, security log analysis and associated industry standard tools. Knowledge and working experience of securing network devices and Windows/UNIX based operating systems. Knowledge of the NAEW&C Programme and NATO E-3A mission system. Prior experience of working in an international environment comprising both military and civilian elements.

### 6. ATTRIBUTES / INTERRELATIONSHIPS

All NAPMA personnel are expected to conduct themselves in accordance with the current NATO Code of Conduct agreed by the North Atlantic Council, and thus display the core values of integrity, impartiality, loyalty, accountability and professionalism.

### 7. COMPETENCIES

The incumbent must demonstrate:

- *Achievement*: Creates own measures of excellence and improves performance;
- *Analytical Thinking*: Sees multiple relationships;
- *Clarity and Accuracy*: Monitors data or projects;
- *Flexibility*: Adapts to unforeseen situations;
- *Impact and Influence*: Takes multiple actions to persuade;
- *Initiative*: Plans and acts up to a year ahead;
- *Organizational Awareness*: Understands organizational climates and culture;
- *Self-Control*: Responds calmly;
- *Conceptual Thinking*: Applies learned concepts;
- *Empathy*: To be open to others' perspectives;
- *Organizational Commitment*: Ability to align own behaviour with the needs, priorities and goals of the Organization.

### 8. REMARKS

Any candidate should be in possession of a NATO Secret (NS) security clearance when taking up the position.

NATO UNCLASSIFIED