



ALLIANCE GROUND SURVEILLANCE (AGS) AND UNCREWED AERIAL SYSTEMS (UAS) PROGRAMME OFFICE, AGS Engineering Branch, Engineering Support Services Section

Technical Officer (Information Assurance)

Grade: 15:A2

Post No.: LQ-128

Original:	English		Clearance:	COSMIC TOP SECRET
Date validated:	06 March 2026		Duty Location:	Capellen, LUX
Validated by:	A. Stoia		Job Code:	A62

SUMMARY

The incumbent reports to the Chief of Section and is responsible for performing all functions related to the Information Security and security accreditation of current and future major Uncrewed Aerial Vehicles (UAV) Systems. More precisely, the incumbent is responsible for performing the following functions:

RESPONSIBILITIES

General Responsibilities

- Participating in Problem Assessment Reports (PAR)/software working groups to provide guidance on software security.
- Reviewing Engineering Change Proposals (ECPs) and Statements of Work (SOWs) and providing security inputs in order to improve the administrative security posture.
- Reviewing Change Request Proposals and providing security assessments.
- Participating to Security Working Groups and act as active member to provide security guidance for ECP.
- Updating the Programme Core System Security documentation for each major ECP [Computer Information Systems description), Community Security Requirement Statement (CSRS), System-Specific Security Requirement Statement (SSRS), System Interconnection Security Requirement Statement (SISRS), Security Test and Verification Plan (STVP), Security Operating Procedures (SecOPs)] and supporting Security Risk Assessment (SRA).
- Maintaining up-to-date security files including special details relating to NATO Personnel and Facility security clearance certificates for all NSPA contractors working for the UAV Programmes and future NSPA contractors.
- Staying up-to-date with security vulnerabilities and more specifically with NATO bulletins and ensuring their corresponding fixes are implemented within the Programme.
- Providing Security Awareness trainings and security updates specific to the Programme and future missions to NATO stakeholders as needed.
- Updating Programme Security accreditation documentation whenever required.
- Performing Travel on Duty (TDY) as required, in accordance with the applicable Civilian Personnel Regulations.
- Performing other related functions as required in peacetime and any other appropriate functions assigned in times of crisis or war.
- In the event of crisis or war the incumbent will, subject to the agreement of their national authorities, remain in the service of the Agency.

Specific Responsibilities

- Implementing, maintaining, controlling and overseeing the secure gateway systems composed of firewalls, application gateways, data guards and diodes (One Identity Safeguard, Infodas Secure Domain Transition (SDoT) and Palo Alto firewall.

- Creating and maintaining Classified Remote connections to Programme stakeholders including the Security Accreditation documentation preparation.
- Drafting ECPs related to security when required.
- Providing support in updating Security Accreditation Strategy, SecOps, System Interconnection Specific Requirement Statements and other security accreditation documents.
- Overseeing contractor work in the domain of system security patches.
- Witnessing security audits when required.
- Ensuring the implementation of the internal control and risk management processes and managing the risks raised in their area of responsibility in compliance with NSPA prescriptive documents on Internal Control and Risk Management.

QUALIFICATIONS

General Qualifications

- A Bachelor's level qualification from a nationally recognised/certified University in a related discipline and 2 years' post-related experience. Alternatively, the lack of a Bachelor's level qualification may be compensated by the demonstration of a candidate's particular abilities or experience that is/are of interest to the Agency, and include at least 6 years' extensive and progressive expertise in duties related to the function of the post.
- Broad technical background in Information Technology (IT) and related Network and Systems Security.
- Ability to multi-task, manage time and work effectively under pressure while producing high-quality products under short-notice deadlines.
- Ability to develop resourceful and effective solutions using office automation systems and software applications, e.g. Microsoft Office Suite (Word, Excel, and PowerPoint).
- Ability and willingness to work rigorously in a multi-functional organization.
- Sound digital literacy with experience in using office automation systems and software applications, e.g. Microsoft Office Suite (Word, Excel, and PowerPoint).

Specific Qualifications

- Extensive experience implementing and managing security gateways, data guards, diodes and other solutions (Palo Alto firewalls, Infodas SDoT, One Identity Safeguard).
- Experience in Cisco Application Centric Infrastructure (ACI), Active Directory and Open Lightweight Directory Access Protocol (OpenLDAP).

LANGUAGE QUALIFICATIONS

- NATO's official languages are English and French. The work of this post requires fluency in English, while working knowledge of French is desirable.

DESIRABLE QUALIFICATIONS

- University degree in computer-, software- or network-engineering, preferably in a field of Security.
- Certifications and/or proven training certificate in the following: Infodas SDoT, One Identity Safeguard, Palo Alto security solutions.
- General knowledge of NATO security regulations and procedures, especially in the field of cryptographic communication equipment and transmission.

PERSONAL CHARACTERISTICS

- Honest, with positive "can-do" attitude and spirit of cooperation, empowering teamwork toward established objectives.
- Passionate and motivated, equipped with strong communication skills, fostering an environment that encourages community involvement and engagement.

- Displays emotional intelligence and self-control. Holds the capacity to remain calm in the face of adversity/conflict; identifies and works to remedy collaborative concerns in accordance with procedural guidelines.
- All NSPA personnel are expected to conduct themselves in accordance with the current NATO Code of Conduct agreed by the North Atlantic Council (NAC), and thus display the core values of integrity, impartiality, loyalty, accountability, and professionalism.

ADDITIONAL INFORMATION

- N/A



BUREAU DE PROGRAMME "CAPACITÉ ALLIÉE DE SURVEILLANCE TERRESTRE (AGS) ET SYSTÈMES AÉRIENS SANS PILOTE (UAS)", Branche "ingénierie AGS", Section "services de soutien en ingénierie"

Responsable technique (assurance de l'information)

Grade : 15:A2

Poste n° : LQ-128

Original :	Anglais	Habilitation :	COSMIC TRÈS SECRET
Date de validation :	6 mars 2026	Lieu d'affectation :	Capellen, LUX
Validé par :	A. Stoia	Code poste :	A62

RÉSUMÉ

Responsable envers le/la chef de section, le/la titulaire exerce toutes les fonctions afférentes à la sécurité de l'information et à l'homologation de sécurité des systèmes importants de véhicules aériens sans pilote (UAV) actuels et futurs. Il/Elle exerce plus précisément les fonctions suivantes :

RESPONSABILITÉS

Responsabilités générales

- participer à des groupes de travail consacrés aux compte rendu d'évaluation des problèmes ainsi qu'aux logiciels afin de fournir des orientations sur la sécurité des logiciels ;
- examiner les propositions de modification technique ainsi que les cahiers des charges et fournir des contributions en matière de sécurité afin d'améliorer la posture de sécurité administrative ;
- examiner les propositions de demande de modification et fournir des évaluations de la sécurité ;
- participer aux groupes de travail consacrés à la sécurité et y contribuer activement afin de fournir des orientations en matière de sécurité concernant les propositions de modification technique ;
- mettre à jour la documentation relative à la sécurité du système central du programme pour chaque proposition de modification technique (descriptions des systèmes d'information et de communication, expression des besoins de sécurité communs, énoncé des besoins de sécurité propres au système, expression des besoins de sécurité applicables à l'interconnexion de systèmes, plan d'essai et d'évaluation de la sécurité, procédures d'exploitation de sécurité) et apporter une aide pour l'évaluation des risques de sécurité ;
- tenir à jour les dossiers de sécurité comprenant des renseignements spécifiques se rapportant aux certificats d'habilitation de sécurité du personnel et des installations OTAN et concernant tous les titulaires de marché de l'Agence travaillant pour les programmes "UAV" ainsi que les futurs titulaires de marché de la NSPA ;
- se tenir informé(e) des vulnérabilités relatives à la sécurité, et plus particulièrement en prenant connaissance des bulletins OTAN, et veiller à ce que les solutions correspondantes soient mises en œuvre au sein du bureau de programme ;
- fournir aux parties prenantes de l'OTAN, selon les besoins, des formations de sensibilisation à la sécurité ainsi que des points de situation sur la sécurité propres au bureau de programme et aux futures missions ;
- mettre à jour la documentation relative à l'homologation de sécurité du bureau de programme chaque fois que cela est nécessaire ;
- effectuer des déplacements de service selon les besoins, conformément au Règlement du personnel civil ;
- exercer d'autres fonctions connexes selon les besoins en temps de paix et toute autre fonction appropriée qui lui sera confiée en période de crise ou en temps de guerre.
- En cas de crise ou de guerre, le/la titulaire restera au service de l'Agence, sous réserve de l'accord de ses autorités nationales.

Responsabilités particulières

- mettre en œuvre, tenir à jour, contrôler et superviser les systèmes de passerelles sécurisées constitués de pare-feu, de passerelles d'application, de gardes de données et de diodes (solution One Identity Safeguard, dispositifs SDoT d'Infodas et pare-feu Palo Alto) ;

- établir et maintenir des connexions à distance de niveau classifié avec les parties prenantes au sein du bureau de programme, notamment en vue d'élaborer la documentation relative à l'homologation de sécurité ;
- rédiger les propositions de modification technique relatives à la sécurité lorsque cela est nécessaire ;
- aider à mettre à jour la stratégie d'homologation de sécurité, les procédures d'exploitation de sécurité, les énoncés des impératifs de sécurité applicables à une interconnexion de systèmes et d'autres documents d'homologation de sécurité ;
- superviser le travail des titulaires de marché dans le domaine des correctifs de sécurité des systèmes ;
- assister à des audits de sécurité selon les besoins ;
- veiller à la mise en œuvre des processus de contrôle interne et de gestion des risques, et gérer les risques signalés dans son domaine de responsabilité conformément aux documents réglementaires de la NSPA relatifs au contrôle interne et à la gestion des risques.

QUALIFICATIONS

Qualifications générales

- Diplôme d'études supérieures de premier cycle dans une discipline pertinente, délivré par un établissement reconnu ou certifié au niveau national, et deux années d'expérience dans un domaine lié au poste. Un(e) candidat(e) peut compenser l'absence de diplôme d'études supérieures de premier cycle s'il/si elle démontre des capacités ou une expérience particulières présentant un intérêt pour l'Agence, assorties de compétences approfondies acquises progressivement (au moins six années durant) dans des fonctions en rapport avec celles de ce poste.
- Vaste expérience technique dans le domaine des systèmes informatiques et de la sécurité des réseaux et des systèmes correspondants.
- Aptitude à mener plusieurs tâches de front, à gérer le temps et à travailler efficacement sous pression tout en fournissant des prestations de grande qualité dans de brefs délais.
- Aptitude à mettre au point des solutions ingénieuses et efficaces en utilisant des systèmes et des logiciels de bureautique [p. ex. la suite Microsoft (MS) Office (Word, Excel et PowerPoint)].
- Capacité et volonté de travailler avec rigueur au sein d'une organisation multifonctionnelle.
- Solide maîtrise des outils numériques assortie d'une expérience de l'utilisation des systèmes et des logiciels de bureautique [p. ex. la suite Microsoft Office (Word, Excel et PowerPoint)].

Qualifications particulières

- Vaste expérience de la mise en œuvre et de la gestion de passerelles de sécurité, de gardes de données, de diodes et d'autres solutions (pare-feu Palo Alto, dispositifs SDoT d'Infodas, solution One Identity Safeguard).
- Expérience des outils Cisco ACI (infrastructure axée sur les applications), Active Directory et OpenLDAP (implémentation libre du protocole LDAP).

CONNAISSANCES LINGUISTIQUES

- Les langues officielles de l'OTAN sont l'anglais et le français. Une bonne maîtrise de l'anglais est nécessaire pour le travail effectué à ce poste, et une connaissance pratique du français est souhaitable.

QUALIFICATIONS SOUHAITABLES

- Diplôme d'études supérieures en ingénierie informatique, logicielle ou réseau, de préférence dans le domaine de la sécurité.
- Certification ou certificat de formation reconnu dans les domaines suivants : solutions de sécurité fournies par SDoT d'Infodas, One Identity Safeguard et Palo Alto.
- Connaissance générale des règles et procédures de sécurité de l'OTAN, en particulier dans le domaine des matériels et de la transmission de communications cryptographiques.

QUALITÉS PERSONNELLES

- Honnêteté, attitude positive et volontaire, et esprit de coopération. Volonté de valoriser le travail d'équipe dans le but de réaliser les objectifs fixés.
- Passion et motivation alliées à une solide aptitude à communiquer, capacité à promouvoir un climat de travail favorisant la participation ainsi que l'engagement des parties prenantes.

- Intelligence émotionnelle et maîtrise de soi. Capacité à garder son calme face à l'adversité ou dans des situations conflictuelles. Aptitude à détecter les difficultés liées au travail en commun et à œuvrer pour y remédier conformément aux procédures.
- Il est attendu de tous les membres du personnel de la NSPA qu'ils se comportent conformément au texte en vigueur du Code de conduite de l'OTAN adopté par le Conseil de l'Atlantique Nord et qu'en conséquence, ils incarnent les valeurs fondamentales que sont l'intégrité, l'impartialité, la loyauté, le sens des responsabilités et le professionnalisme.

INFORMATIONS COMPLÉMENTAIRES

- S.O.