NATO Support and Procurement Agency (NSPA)

CORPORATE MANAGEMENT AND OVERSIGHT OFFICE, Chief Security Office, MMF Security Office

Technician (MMF CIS Security)

Grade: 12:B5

Post No.: AX-35

Original:	English	|	*Clearance:*	COSMIC TOP SECRET
Date validated:	06 March 2026	|	*Duty Location:*	Cologne-Wahn, DEU
Validated by:	A. Stoia	|	*Job Code:*	A642

SUMMARY

The incumbent reports to the Senior Security Officer (MMF) and is responsible for Communication Information Systems Security (CISS), in accordance with NATO, NATO Support and Procurement Organisation (NSPO)/NSPA and the Multinational Multi Role Tanker Transport Fleet (MMF) prescriptive documents, and providing daily security support to the Multinational Multi Role Tanker Transport Unit (MMU) Forward Operating Base (FOB+) at Cologne-Wahn, DEU. More precisely, the incumbent is responsible for executing the following tasks:

RESPONSIBILITIES

General Responsibilities

- Acting as a Communication Security (COMSEC) specialist for MMU FOB+ location.
- Assisting the MMF FOB+ COMSEC Officer with CRYPTO operations, coordination, training and awareness.
- Ensuring the System-Specific Security Requirement Statements (SSRS) for all MMU systems and stand-alone Communication and Information Systems (CIS) of the MMU FOB+ are up-to-date and follow the applicable NATO, NSPO/NSPA and public rules and regulations.
- Ensuring the CIS security level complies with the requirements of NATO, NSPO/NSPA, and MMU.
- Providing CISS related assistance and advice to the MMU FOB+ CIS Operating Authority, system administrators, and users, to include functional and technical CISS specifications for projects deriving from business requirements.
- Executing CISS inspections of the systems at MMU FOB+ location, in order to control and check that classified electronic information is properly stored, processed, transmitted and safeguarded, whose results are to be forwarded in writing to the Security Officer (MMF) of FOB+ as required.
- Planning and executing relevant CISS and CRYPTO related training and awareness for all MMU personnel, as required.
- Informing the Security Officer (MMF) of FOB+ of any system/network security loopholes, infringements and vulnerabilities or incidents which may come to light, and leading local CIS security investigations.
- Assisting with the coordination and execution of security accreditation/reaccreditation tasks for all MMU local classified CIS in accordance with NATO policy, supporting directives and Security Accreditation Authority (SAA) requirements and guidance.
- Assisting with the coordination of the execution of risk analysis and/or vulnerability assessments of MMU FOB+ local CIS (with automated tools as applicable) to identify CIS vulnerabilities and threats.
- Issuing certificates of security clearances.
- Establishing and maintaining the MMU FOB+ database providing access to MMU FOB+ personnel, and contractors.
- Assisting in establishing and maintaining the Security Education and Awareness Programme and delivering the security education and awareness briefings.

- Preparing courier certificates for the transmission of classified documents and material.
- Checking and maintaining all inventories of classified NATO Restricted (NR) and NATO Secret (NR) documents held by MMU at MMU FOB+ location.
- Monitoring the classified material destruction procedure and coordinating operations with the person in charge of the Registry.
- Ensuring the relevant physical security regulations are implemented such as access to restricted areas, change of safe combinations or random checking of the clear desk policy.
- Assisting in the coordination of issues with the Cologne-Wahn air base Security.
- Providing usual security briefings and maintaining records of Privately Owned Portable Computer equipment.
- Executing other related tasks as required in peacetime and any other appropriate tasks 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

- Assisting in formulating and maintaining Security Operating Procedures (SecOPs) for all MMU FOB+ CIS, and circulating the SecOPs to system/network administrators and users on a periodic basis.
- Approving access and maintaining a record of all persons authorized to any part of the MMU FOB+ CIS and the extent of their authorisation.
- Monitoring security-relevant activities, duties and responsibilities of the system administrator, and checking audit information for event/process failure, and unauthorised user and system activity.
- Checking the implementation and maintenance of hardware, firmware and software modifications and enhancements to the CIS to ensure security is maintained.
- Ensuring the proper custody of classified computer storage media and other CIS machine- or human-readable documents.
- Ensuring CIS elements and external mass storage media (EMSM) are properly controlled and marked with security classification.
- Ensuring contractors or other organisations receiving classified computer storage media have the appropriate security provisions in place and need-to-know for the information, in accordance with the requirements of NATO Security Policy and its supporting directives.
- Ensuring system/network security relevant information is properly backed up and recovery procedures are in place.
- Checking the configuration management aspects of changes to security-related hardware, firmware or software and associated documentation.
- Ensuring the implementation and maintenance of the security provisions applicable to those areas of the site(s) hosting elements of the CIS.
- Assisting the Senior Security Officer (MMF) of MOB in replacing the Security Officer (MMF) of FOB+ in case of absence.

QUALIFICATIONS

General Qualifications

- Higher vocational training in a relevant discipline and 3 years' post-related experience. Acceptable alternatives: secondary education and 5 years' post-related experience, or an equivalent education combined with an appropriate amount of relevant, professional experience.
- Ability to be self-motivated, to work independently, under stress and tight deadlines.
- Well-developed communication skills (written, oral and presentation).

- Good knowledge of and experience in INFOSEC regulations and practices within NATO or in a similar organisation.
- Sound digital literacy with experience in using office automation systems and software applications, e.g. Microsoft Office Suite (Word, Excel, and PowerPoint).

Specific Qualifications

- A CIS Security, IT Security, Information Security or Communication Security certified training from NATO or National Security Department or equivalent commercial IT Security training companies.
- Knowledge of NATO COMSEC and Computer Security (COMPUSEC) principles and their application to the development of effective CISS programmes.
- Good knowledge of and experience in Risk Analysis and management methodologies.
- Experience in planning and executing CISS or IT related training.

LANGUAGE QUALIFICATIONS

- NATO's official languages are English and French. However, the work of this post is conducted in English and therefore fluency in that language is essential.

DESIRABLE QUALIFICATIONS

- Good understanding of the underlying concepts of CIS/IT service management and delivery.
- Additional educational background in IT or IT security or computer science.
- Knowledge of COMPUSEC principles and their application to the development of effective CISS programmes.

PERSONAL CHARACTERISTICS

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

Agence OTAN de Soutien et d'Acquisition (NSPA)

BUREAU "GESTION ET SUPERVISION D'ENTREPRISE", Bureau du responsable en chef de la sécurité, Bureau de la sécurité de la MMF

Technicien(ne) [MMF / sécurité des SIC]

Grade : 12:B5

Poste n° : AX-35

Original :	Anglais	|	*Habilitation :*	COSMIC TRÈS SECRET
Date de validation :	6 mars 2026	|	*Lieu d'affectation :*	Cologne-Wahn, DEU
Validé par :	A. Stoia	|	*Code poste :*	A642

RÉSUMÉ

Sous la direction du/de la responsable principal(e) de sécurité (MMF), le/la titulaire est chargé(e) de la sécurité des systèmes d'information et de communication (SIC), conformément aux documents réglementaires de l'OTAN, de l'Organisation OTAN de soutien et d'acquisition (NSPO) et de la NSPA ainsi que de la flotte multinationale d'avions multirôles de ravitaillement en vol et de transport (MMF). Il/Elle fournit un soutien quotidien en matière de sécurité à la base d'opérations avancée (FOB+) de l'Unité multinationale "avions multirôles de ravitaillement en vol et de transport" (MMU) située à Cologne-Wahn, en Allemagne. Il/Elle exécute plus précisément les tâches suivantes :

RESPONSABILITÉS

Responsabilités générales

- exercer les fonctions de spécialiste de la sécurité des communications (COMSEC) pour la base FOB+ de la MMU ;
- aider le/la responsable COMSEC de la base FOB+ de la MMF pour ce qui concerne l'exploitation, la coordination, la formation et le maintien des connaissances en matière de systèmes cryptographiques ;
- veiller à ce que les énoncés des besoins de sécurité propres aux systèmes soient à jour pour l'ensemble des systèmes de la MMU et des SIC autonomes de la base FOB+ de la MMU, et à ce qu'ils soient conformes à la réglementation publique en vigueur, ainsi qu'à celle de l'OTAN, de la NSPO et de la NSPA ;
- veiller à ce que le niveau de sécurité des SIC soit conforme aux exigences de l'OTAN, de la NSPO, de la NSPA et de la MMU ;
- fournir, en ce qui concerne la sécurité des SIC, une aide et des avis aux autorités responsables de la mise en œuvre des SIC de la base FOB+ de la MMU, aux administrateurs de systèmes et aux utilisateurs, ce qui comprend les spécifications fonctionnelles et techniques relatives à la sécurité des SIC au titre de projets découlant de besoins opérationnels ;
- effectuer des inspections de sécurité des SIC sur la base FOB+ de la MMU, de manière à contrôler et vérifier que les informations électroniques classifiées sont correctement stockées, traitées, transmises et sauvegardées, inspections dont les résultats doivent être communiqués par écrit à l'officier de sécurité (MMF) de la base FOB+ selon les besoins ;
- programmer et dispenser des formations appropriées et des actions de sensibilisation portant sur la sécurité des SIC et les systèmes cryptographiques pour l'ensemble du personnel de la MMU, en fonction des besoins ;
- informer l'officier de sécurité (MMF) de la base FOB+ de toute faille, violation ou faiblesse relatives à la sécurité et de tout incident qui se produirait dans les systèmes et les réseaux, et mener des enquêtes locales de sécurité des SIC ;
- aider à coordonner et à réaliser des tâches d'homologation ou de renouvellement d'homologation de sécurité concernant tous les SIC locaux classifiés de la MMU, conformément à la politique générale de l'OTAN, aux directives complémentaires et aux exigences et orientations des autorités d'homologation de sécurité ;
- aider à coordonner l'exécution de l'analyse des risques ou des évaluations de vulnérabilité des SIC locaux de la base FOB+ de la MMU (à l'aide d'outils automatisés s'il y a lieu) afin d'identifier les vulnérabilités des SIC et les menaces auxquelles ils sont soumis ;
- délivrer des certificats d'habilitation de sécurité ;
- créer et tenir à jour la base de données de la base FOB+ de la MMU répertoriant les droits d'accès accordés au personnel de ladite base et aux titulaires de marché ;
- aider à élaborer et à tenir à jour le programme de formation et de sensibilisation à la sécurité, et présenter des exposés sur ce programme ;

- établir des ordres de mission de messager pour la transmission de documents et de matériels classifiés ;
- vérifier et tenir à jour tous les inventaires des documents classifiés (NATO DIFFUSION RESTREINTE et NATO SECRET) détenus par la MMU sur sa base FOB+ ;
- suivre la procédure de destruction des matériels classifiés et coordonner les opérations avec la personne responsable du bureau d'ordre ;
- veiller à ce que les règles de sécurité physique appropriées soient mises en œuvre, comme celles concernant l'accès à des zones à accès limité, le changement des combinaisons de coffre ou les contrôles aléatoires du respect de la politique en matière de mise en sécurité des documents ;
- aider à la coordination des questions avec les services chargés de la sécurité de la base aérienne de Cologne-Wahn ;
- présenter les exposés habituels sur la sécurité et tenir des registres de matériels informatiques portables qui appartiennent à des particuliers ;
- exécuter d'autres tâches connexes selon les besoins en temps de paix et toute autre tâche 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

- aider à rédiger et à tenir à jour les procédures d'exploitation de sécurité (SecOPs) pour l'ensemble des SIC de la base FOB+ de la MMU et communiquer ces SecOPs périodiquement aux administrateurs et aux utilisateurs des systèmes et des réseaux ;
- approuver les accès et tenir un registre de toutes les personnes autorisées à accéder à toute partie des SIC de la base FOB+ de la MMU, en précisant l'étendue de cette autorisation ;
- superviser, lorsqu'elles sont applicables à la sécurité, les activités, les fonctions et les responsabilités de l'administrateur(-trice) systèmes, et vérifier les informations d'audit relatives aux incidents et aux défaillances dans les processus, ainsi qu'aux activités non autorisées des utilisateurs et des systèmes ;
- vérifier la mise en œuvre et la maintenance des modifications et améliorations des matériels, des micrologiciels et des logiciels des SIC afin de s'assurer que la sécurité n'est pas compromise ;
- veiller à la bonne conservation des supports de stockage informatique classifiés et d'autres documents SIC lisibles par machine ou par un(e) utilisateur(-trice) ;
- veiller à ce que les éléments des SIC et les supports de stockage de masse externes soient contrôlés de manière appropriée et comportent un marquage précisant le niveau de classification de sécurité ;
- veiller à ce que les titulaires de marché ou autres organismes destinataires de supports de stockage informatique classifiés aient en place des dispositions de sécurité et à ce qu'ils aient le besoin d'en connaître, conformément aux exigences de la politique de sécurité de l'OTAN et de ses directives complémentaires ;
- veiller à ce que les informations ayant une incidence sur la sécurité des systèmes et des réseaux soient correctement sauvegardées et à ce que des procédures de récupération soient en place ;
- vérifier les aspects relatifs à la gestion de la configuration des modifications des matériels, micrologiciels ou logiciels liés à la sécurité, ainsi que de la documentation connexe ;
- veiller à la mise en œuvre et à la tenue à jour des dispositions relatives à la sécurité qui s'appliquent aux zones du ou des sites où sont installés des éléments des SIC ;
- aider le/la responsable principal(e) de sécurité (MMF) de la base d'opérations principale à remplacer l'officier de sécurité (MMF) de la base FOB+ en cas d'absence.

QUALIFICATIONS

Qualifications générales

- Formation professionnelle supérieure dans une discipline pertinente assortie de trois ans d'expérience en lien avec le poste. Autres formations ou expérience acceptables : études secondaires assorties de cinq ans d'expérience en lien avec le poste, ou formation équivalente combinée à une expérience professionnelle suffisante et pertinente.
- Aptitude à se motiver et à travailler de façon indépendante, sous pression et sous la contrainte de délais serrés.
- Compétences bien établies en matière de communication (par écrit, à l'oral et lors d'exposés).

- Bonne connaissance des pratiques et règlements relatifs à la sécurité des informations et expérience acquise dans ce domaine au sein de l'OTAN ou dans un organisme similaire.
- 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

- Une formation certifiée dans le domaine de la sécurité des SIC, de la sécurité informatique, de la sécurité des informations ou de la sécurité des communications dispensée par l'OTAN ou un département national de la sécurité ou par des entreprises de formation en matière de sécurité informatique.
- Connaissance des principes de COMSEC et de sécurité informatique de l'OTAN ainsi que de leur application dans la mise au point de programmes efficaces de sécurité des SIC.
- Bonne connaissance et expérience des méthodes d'analyse et de gestion de risques.
- Expérience de la planification et de l'exécution de formations dans les domaines de la sécurité des SIC ou de l'informatique.

CONNAISSANCES LINGUISTIQUES

- Les langues officielles de l'OTAN sont l'anglais et le français. Toutefois, la langue de travail à ce poste étant l'anglais, il est essentiel d'avoir une bonne maîtrise de cette langue.

QUALIFICATIONS SOUHAITABLES

- Bonne compréhension des concepts sur lesquels s'appuient la gestion et la fourniture de services SIC ou informatiques.
- Formation complémentaire en technologies de l'information, en sécurité informatique ou en informatique.
- Connaissance des principes de sécurité informatique de l'OTAN ainsi que de leur application dans la mise au point de programmes efficaces de sécurité des SIC.

QUALITÉS PERSONNELLES

- 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.
- Honnêteté, attitude positive et volontaire, et esprit de coopération. Capacité à 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.
- 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.