NATO Support and Procurement Agency (NSPA)

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

CIS and COMSEC Officer

Grade: 15:A2

Post No.: AX-50

Original:	English	|	*Clearance:*	NATO SECRET
Date validated:	30 March 2026	|	*Duty Location:*	Pápa, HUN
Validated by:	A. Stoia	|	*Job Code:*	A62

SUMMARY

The incumbent reports to the Senior Security Officer and is responsible for the delivery of Communication and Information System (CIS) Security responsibilities and routine coordination of CIS Security (CISS) and Communications Security (COMSEC) functional outputs for the Strategic Airlift Capability (SAC) Programme. The incumbent is primarily responsible for CISS and COMSEC oversight, management and support including security accreditation, investigations, digital forensic and auditing, inspections as well as CISS and COMSEC training and awareness. More precisely, the incumbent is responsible for performing/executing the following functions/tasks:

RESPONSIBILITIES

General Responsibilities

- Supporting the Senior Security Officer in providing CISS and COMSEC advice to the organization's leadership and other stakeholders.
- Supporting the Senior Security Officer in the development and implementation of the SAC Programme internal CISS and COMSEC regulations, as well as in contributing to the development of NSPA CISS Policies.
- Acting as the CIS Security Officer for designated CIS and for all SAC Programme organizational elements, as required.
- Supporting and coordinating, as required, the Security Accreditation (SA) processes of all SAC Programme CIS and other electronic or Internet of Things (IoT) systems requiring security accreditation.
- Acting as the COMSEC Officer for designated CRYPTO accounts and providing COMSEC related support as required.
- Deputizing for the Senior Security Officer, as required, in case of their absence, and in line with the NATO Civilian Personnel Regulations (NCPR).
- Developing, executing, evaluating and adapting a SAC Programme CIS Security Training and Awareness Programme (including online computer-based trainings/courses, briefings, posters/leaflets, intranet and email newsletters etc.).
- Taking lead in coordinating timely response to CISS infractions and incidents reported to Security Office (SAC), or providing necessary contributions (including provision of Digital Forensics) to CISS or other investigations as required.
- Developing and leading digital forensic capability in support of CISS Insider Threat Programme and other various investigatory requirements.
- Planning and providing CISS and COMSEC on-demand bespoke training and awareness sessions, to SAC Programme personnel and contractors.
- Developing and maintaining capability, in accordance with NATO and NSPA CISS regulations, to monitor users' and system administrators' access to sensitive or classified information, with the aim of detecting excessive permissions (overcrossing need-to-know boundaries), and mitigating the risk of data breach or leakage.
- Assisting in planning, organizing and exercising applicable CISS activities, providing overall direction and guidance on the implementation, operation and support of required CISS measures and tools.

- Developing and implementing an Annual Plan for inspecting the operational status and usage of the physical security infrastructure protecting the CIS installations (e.g. data centers, network distribution rooms, cabling etc.) and reporting and/or taking appropriate action as required.
- Assuring that Security Operating Procedures (SecOPs) for all SAC Programme CIS, are circulated to system/network administrators and users, and maintaining CISS awareness of system/network administrators and users.
- Ensuring that all SAC Programme CIS security accreditation documents [e.g. System Specific Requirement Statements (SSRS), etc.] are up to date and in line with relevant regulations.
- Staying abreast of technological developments relevant to the area of work.
- 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

- Conducting CISS oversight by performing periodic checks, inspections and security implementation verifications of SAC Programme CIS to assure compliance with NATO Security Policy and supporting prescriptive documents.
- Designing, implementing and maintaining necessary tools and repositories to process and record necessary information regarding CISS incidents and investigations. This shall include reporting on KPI statistics and assure data is preserved and archived accordingly with policy regulations.
- Coordinating security accreditation (SA) processes with Security Accreditation Authorities (SAA), including formulation, verification and revision of SA documentation and its timely submission.
- Identifying, collecting, acquiring and preserving potential digital evidence from SAC Programme CIS resulting from CISS incidents and preserving its integrity, authenticity and admissibility in accordance with relevant legal and security policy requirements.
- Responding to / or providing CISS support to CIS/Cyber Security incidents response/management in line with the applicable NATO CIS Security Incident Management procedures.
- Leading CISS, or contributing to security and other, investigations including provision of Digital Forensic support as necessary.
- Providing digital forensic support to the NSPA investigation function as required.
- Supporting and overseeing the management of CIS SA and Security Risks Assessment (SRA) and reporting on status of all SAC Programme CIS in use (in a form of written report) annually.
- Assisting in planning and executing relevant CISS and Crypto-related training for all SAC Programme personnel and contractors to improve security awareness of staff on CISS and COMSEC matters.
- Providing guidance on CIS Security T&A and accreditation requirements for all SAC Programme CIS and other electronic or IoT systems and overseeing their implementation and CISS compliance.
- Overseeing and advising on the definition, implementation, and regular testing of Business Continuity and Disaster Recovery requirements for the CIS in accordance with the objectives of the organization’s BCP.
- Assisting in ensuring the proper custody of classified computer storage media and other CIS machine- or human-readable documents; carrying out spot checks and maintaining records of checks, at agreed intervals, on the presence of classified computer storage media and on the accuracy of their markings.
- Ensuring security-related logs, including those related to event/process failure and authorized/unauthorized users’ and system activities, are monitored and audited regularly.
- Ensuring that contractors or other organizations 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.
- Controlling, by performing random security inspections of CIS security-related activities, the duties and responsibilities of CIS system administrators.
- In coordination with IT, checking CISS audit information for security event/process failures, and unauthorized user and system activities.

- Ensuring the implementation and maintenance of the physical security provisions applicable to those areas of the site(s) hosting elements of the CIS.
- Assisting in establishing, implementing and reviewing SAC Programme Instructions and Procedures and controlling compliance.
- Providing the lead in supervising processes for the disposal/destruction of classified IT material [Hard Disk Drives (HDDs), etc.].

QUALIFICATIONS

General Qualifications

- University degree in Computer or Information Science, Cyber Security, Security Engineering, Information Assurance, Information and Communication Technologies, or equivalent field education.
- A Bachelor's level qualification from a nationally recognised/certified University in a related discipline and 4 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.
- Very good knowledge of and experience in a broad range of CISS and Cyber Security disciplines within the Agency, a similar organization, or a governmental institution requiring similarly high-level security requirements.
- Very good knowledge of and experience in planning and execution of CIS/Cyber Security Training & Awareness at the organizational level.
- Very good knowledge in CIS/Information and Communication Technologies (ICT) security concepts and methodologies, combined with a very good understanding of underlying technical aspects.
- Ability to multi-task, manage time and work effectively under pressure while producing high-quality products under short-notice deadlines.
- Sound digital literacy with experience in using office automation systems and software applications, e.g. Microsoft Office Suite (Word, Excel, and PowerPoint).

Specific Qualifications

- Knowledge and experience in CIS/IT System engineering, implementation and/or administration.
- Firm knowledge of CIS/Cyber Security and digital Forensic principles, and their application.
- Knowledge and experience in the area of CIS/ICT Security Risk Assessment and Management methodologies.
- Practice in writing security documentation in relation to security policies, security accreditation and training and awareness.
- Good knowledge and work experience in CIS/ICT security accreditation, testing and inspections or auditing.
- Experience in planning and delivering CIS Security-related training.
- Demonstrated ability to write clear and concise investigative reports and effectively communicate technical information.

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

- Very good knowledge of NATO Security Policy and supporting directives.
- NATO CIS Security / COMSEC Courses.
- A Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), or other widely recognized CIS/IT or Cyber Security certification.

- Very good knowledge of and experience in a broad range of CISS, Cyber Security and digital forensic disciplines, regulations and practices within NATO or similar organization or governmental institution requiring equivalent high security requirements.

PERSONAL CHARACTERISTICS

- Autonomy in delivering results and managing tasks in a fast-paced environment.
- 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 SAC

Responsable SIC et COMSEC

Grade : 15:A2

Poste n° : AX-50

Original :	Anglais	|	*Habilitation :*	NATO SECRET
Date de validation :	30 mars 2026	|	*Lieu d'affectation :*	Pápa, HUN
Validé par :	A. Stoia	|	*Code poste :*	A62

RÉSUMÉ

Sous la direction du/de la responsable principal(e) de sécurité, le/la titulaire exerce des responsabilités en matière de sécurité des systèmes d'information et de communication (SIC) et assure la coordination régulière des activités fonctionnelles en matière de sécurité des SIC et de sécurité des communications (COMSEC) pour le programme de la Capacité de transport aérien stratégique (SAC). Il/Elle est principalement responsable de la surveillance, de la gestion et du soutien en matière de sécurité des SIC et de COMSEC, ce qui comprend l'homologation de sécurité, la réalisation d'enquêtes, d'audits et d'inspections, la criminalistique numérique ainsi que la formation et la sensibilisation en matière de sécurité des SIC et de COMSEC. Plus précisément, le/la titulaire exerce les fonctions et exécute les tâches suivantes :

RESPONSABILITÉS

Responsabilités générales

- aider le/la responsable principal(e) de sécurité à fournir des conseils en matière de sécurité des SIC et de COMSEC à la direction de l'organisation et à d'autres parties prenantes ;
- aider le/la responsable principal(e) de sécurité à élaborer et à mettre en œuvre les règlements internes en matière de sécurité des SIC et de COMSEC du programme SAC, ainsi qu'à contribuer à l'élaboration des politiques générales de la NSPA en matière de sécurité des SIC ;
- faire fonction de responsable de la sécurité des SIC pour les services chargés des SIC et tous ceux du programme SAC qui lui sont confiés, s'il y a lieu ;
- assurer le soutien et la coordination, selon les besoins, des processus d'homologation de sécurité de tous les SIC du programme SAC et d'autres systèmes électroniques ou liés à l'Internet des objets nécessitant une telle homologation ;
- faire fonction de responsable COMSEC pour les comptes cryptographiques qui lui sont confiés et fournir un soutien en matière de COMSEC selon les besoins ;
- suppléer le/la responsable principal(e) de sécurité, selon les besoins, en cas d'absence et conformément au Règlement du personnel civil de l'OTAN ;
- élaborer, exécuter, évaluer et adapter un programme de formation et de sensibilisation à la sécurité des SIC destiné au programme SAC (ce qui comprend des formations ou des cours en ligne assistés par ordinateur, des présentations, des affiches ou des dépliants, l'intranet et des bulletins électroniques, etc.) ;
- piloter la coordination visant à apporter en temps utile des réponses aux infractions et aux incidents relevant de la sécurité des SIC signalés au Bureau de la sécurité de la SAC, ou apporter les contributions nécessaires (ce qui comprend la fourniture de services de criminalistique numérique) pour ce qui concerne les enquêtes liées à la sécurité des SIC ou autres, selon les besoins ;
- développer et diriger une capacité de criminalistique numérique en appui du programme relatif aux menaces internes en matière de sécurité des SIC et d'autres besoins divers relatifs aux enquêtes ;
- planifier et dispenser des séances de formation et de sensibilisation en matière de sécurité des SIC et de COMSEC, à la demande et personnalisées, au personnel du programme SAC et aux titulaires de marché ;
- mettre au point et maintenir une capacité (conformément aux règlements de l'OTAN et de la NSPA en matière de sécurité des SIC) permettant de contrôler l'accès des utilisateurs et des administrateurs système aux informations sensibles ou classifiées, dans le but de détecter les autorisations abusives (débordant des limites du besoin d'en connaître) et d'atténuer le risque de compromission ou de fuite de données ;
- aider à planifier, à organiser et à réaliser des activités dans le domaine de la sécurité des SIC ainsi que fournir des directives et des orientations générales sur la mise en œuvre, l'exploitation et le soutien des mesures et des outils nécessaires à la sécurité des SIC ;

- élaborer et mettre en œuvre un plan annuel visant à contrôler l'état de fonctionnement et l'utilisation de l'infrastructure physique de sécurité qui protège les installations SIC (p. ex. centres de traitement de données, salles de distribution réseau, câblage, etc.) et rendre compte ou prendre les mesures appropriées selon les besoins ;
- veiller à ce que les procédures d'exploitation de sécurité pour l'ensemble des SIC du programme SAC soient communiquées aux administrateurs des systèmes ou des réseaux ainsi qu'aux utilisateurs, et à ce que ceux-ci restent sensibilisés à la sécurité des SIC ;
- veiller à ce que tous les documents relatifs aux homologations de sécurité des SIC du programme SAC (p. ex. les énoncés des besoins spécifiques des systèmes) soient tenus à jour et conformes à la réglementation applicable en la matière ;
- se tenir au courant des nouveautés technologiques dans son domaine d'activité ;
- 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

- mener une supervision en matière de sécurité des SIC en effectuant périodiquement des contrôles, des inspections et des vérifications concernant le respect des mesures de sécurité sur les SIC du programme SAC de façon à garantir la conformité avec la politique de sécurité de l'OTAN et les documents réglementaires correspondants ;
- concevoir, mettre en œuvre et maintenir les outils et les répertoires nécessaires pour traiter et enregistrer les informations requises portant sur les incidents et les enquêtes en matière de sécurité des SIC, ce qui comprend le fait de rendre compte des statistiques relatives aux indicateurs clés de performance et de veiller à ce que les données soient préservées et archivées conformément aux règlements applicables ;
- coordonner les processus d'homologation de sécurité avec les autorités compétentes en la matière, ce qui comprend l'établissement, la vérification et la révision des documents liés à l'homologation de sécurité et leur soumission en temps voulu ;
- déceler, recueillir, acquérir et conserver les preuves numériques éventuelles provenant des SIC du programme SAC à la suite d'incidents relevant de la sécurité des SIC et préserver leur intégrité, leur authenticité et leur admissibilité conformément aux exigences juridiques et découlant des politiques de sécurité applicables ;
- intervenir ou fournir un soutien en matière de sécurité des SIC dans le contexte de la réponse à des incidents liés aux SIC ou à la cybersécurité, ou de la gestion de ces incidents, conformément aux procédures de l'OTAN applicables en la matière ;
- piloter des enquêtes sur la sécurité des SIC, ou contribuer à celles portant sur la sécurité et sur d'autres domaines, ce qui comprend la fourniture, selon les besoins, d'un soutien en matière de criminalistique numérique ;
- fournir un soutien en matière de criminalistique numérique à la fonction d'enquête de la NSPA selon les besoins ;
- soutenir et superviser la gestion de l'homologation de sécurité des SIC et de l'évaluation des risques de sécurité, et rendre compte chaque année de la situation de tous les SIC utilisés par le programme SAC (sous la forme d'un rapport écrit) ;
- aider à programmer et à dispenser les formations appropriées portant sur la sécurité des SIC et sur les systèmes cryptographiques pour tous les membres du personnel du programme SAC ainsi que pour les titulaires de marché afin d'améliorer leur niveau de sensibilisation en matière de sécurité des SIC et de COMSEC ;
- fournir des orientations concernant les formations et les actions de sensibilisation relatives à la sécurité des SIC ainsi que sur les besoins en matière d'homologation pour l'ensemble des SIC du programme SAC et pour d'autres systèmes électroniques ou liés à l'Internet des objets, et contrôler leur mise en œuvre et leur conformité en matière de sécurité des SIC ;
- superviser la définition, la mise en œuvre et le test régulier des exigences en matière de continuité des activités et de plans de reprise après sinistre concernant les SIC et fournir des conseils à ce sujet, conformément aux objectifs liés à la planification de la continuité des activités de l'organisation ;
- aider à veiller à ce que les supports de stockage informatique classifiés et d'autres documents SIC lisibles par machine ou par des utilisateurs soient bien conservés ; effectuer des contrôles ponctuels et établir des relevés, à intervalles convenus, concernant la présence de supports de stockage informatique classifiés et l'exactitude de leur marquage ;
- veiller à ce que les journaux relatifs à la sécurité, dont ceux concernant les incidents ou les défaillances dans les processus ainsi que les activités autorisées ou non des utilisateurs et des systèmes, fassent l'objet d'un suivi et d'audits réguliers ;
- veiller à ce que les titulaires de marché ou les autres organismes auxquels sont confiés des supports de stockage informatique classifiés aient mis en place les dispositions de sécurité appropriées et qu'ils aient le besoin de connaître les informations concernées, conformément aux exigences de la politique de sécurité de l'OTAN et de ses directives complémentaires ;
- contrôler, en menant des inspections de sécurité aléatoires des activités liées à la sécurité des SIC, les fonctions et responsabilités exercées par les administrateurs des SIC ;
- en coordination avec la Division "applications informatiques et accords sur le niveau de service" (IT), vérifier les informations d'audit de sécurité des SIC relatives aux événements de sécurité ou aux défaillances des processus correspondants, ainsi qu'aux activités non autorisées des utilisateurs et des systèmes ;

- veiller à la mise en œuvre et à la tenue à jour des dispositions relatives à la sécurité physique qui s'appliquent aux zones du ou des sites où sont installés des éléments des SIC ;
- aider à établir, mettre en œuvre et revoir les instructions et les procédures du programme SAC, et en contrôler la conformité ;
- piloter la supervision des processus relatifs à l'élimination ou à la destruction de matériels informatiques classifiés (disques durs, etc.).

QUALIFICATIONS

Qualifications générales

- Diplôme d'études supérieures en informatique ou en sciences de l'information, cybersécurité, ingénierie en matière de sécurité, assurance de l'information, technologies de l'information et de la communication (TIC), ou formation professionnelle équivalente.
- Diplôme d'études supérieures de premier cycle dans une discipline pertinente, délivré par un établissement reconnu ou certifié au niveau national, et quatre 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 qui présentent un intérêt pour l'Agence, assorties de connaissances approfondies acquises progressivement (au moins six années durant) dans des fonctions liées à ce poste.
- Très bonne connaissance et expérience d'un large éventail de disciplines relatives à la sécurité des SIC et à la cybersécurité au sein de l'Agence, d'un organisme similaire ou d'une institution gouvernementale imposant des exigences de sécurité élevées similaires.
- Très bonne connaissance et expérience de la planification et de l'exécution d'activités de formation et d'actions de sensibilisation relatives aux SIC et à la cybersécurité au niveau organisationnel.
- Très bonne connaissance des concepts et des méthodes en matière de sécurité des SIC et des TIC, associée à une très bonne compréhension des aspects techniques sous-jacents.
- 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.
- 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

- Connaissance et expérience de l'ingénierie, de la mise en œuvre ou de l'administration de systèmes SIC ou informatiques.
- Solide connaissance des principes de sécurité des SIC, de cybersécurité et de criminalistique numérique ainsi que de leurs applications.
- Connaissance et expérience des méthodes d'évaluation et de gestion des risques touchant la sécurité des SIC ou des TIC.
- Expérience de la rédaction de documents sur la sécurité en rapport avec les politiques de sécurité, l'homologation de sécurité, la formation et la sensibilisation en la matière.
- Bonne connaissance et expérience professionnelle de l'homologation, des tests et des inspections ou de l'audit en matière de sécurité des SIC et des TIC
- Expérience de la planification et de la tenue de formations liées à la sécurité des SIC.
- Aptitude reconnue à rédiger des rapports d'enquête clairs et concis et à communiquer efficacement des informations techniques.

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

- Très bonne connaissance de la politique de sécurité de l'OTAN et de ses directives complémentaires.
- Formations de l'OTAN en matière de sécurité des SIC ou de COMSEC.
- Certificat de professionnel certifié de la sécurité des systèmes d'information, de pirate informatique éthique certifié ou autre certification largement reconnue en matière de sécurité des SIC, d'informatique ou de cybersécurité.

- Très bonne connaissance et très grande expérience dans une large gamme de domaines, de règlements et de pratiques liés à la sécurité des SIC, à la cybersécurité et à la criminalistique numérique au sein de l'OTAN, d'un organisme similaire ou d'une institution gouvernementale imposant des exigences de sécurité aussi élevées.

QUALITÉS PERSONNELLES

- Capacité à atteindre des résultats et à gérer des tâches de manière autonome dans un environnement caractérisé par un rythme de travail rapide.
- 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.