NATO Support and Procurement Agency (NSPA)

CORPORATE MANAGEMENT AND OVERSIGHT OFFICE, Chief Security Office, Communication and Information Systems (CIS) Security Office

Junior Technician (CIS Security)

Grade: 10:B4

Post No.: AX-28

Original:	English	|	*Clearance:*	COSMIC TOP SECRET
Date validated:	04 June 2026	|	*Duty Location:*	Capellen, LUX
Validated by:	A. Stoia	|	*Job Code:*	A642

SUMMARY

The incumbent reports to the Security Manager (CIS and COMSEC) and is responsible for efficiently handling a wide range of operational support duties of an administrative, CIS/Cyber security and organisational nature at office-level. More precisely, the incumbent is responsible for performing the following functions:

RESPONSIBILITIES

General Responsibilities

- Implementing, configuring and maintaining all Chief Security Office's technical CIS/Cyber security, forensic or other security equipment ensuring its availability and continuous operation.
- Designing, implementing and maintaining, in coordination and support of Information and Communications Technology (ICT), databases, spreadsheets, tracking systems, and other digital tools or process workflows being used within CIS Security (CISS) Office.
- Managing and organizing Office documents including filing, scanning, and maintaining electronic records and procedures to ensure required work efficiency.
- Assisting the CISSM in monitoring Office workload and coordinating Office staff leave synchronization, ensuring necessary coverage maintaining processes and operations continuity.
- Supporting operations, planning and coordinating activities of the CIS Security Office as required by CISSM.
- Monitoring timely execution of Office tasks and coordinating priorities adaptation to manage time-sensitive requests.
- In liaison with the Security Manager (CIS and COMSEC) and Officers, collecting and analysing information related to CIS/Cyber security incidents and violations to conduct trend analysis supporting continuous improvement process.
- Compiling and disseminating regular reports, presentations and other cyber security literature as required.
- Liaising and collaborating with relevant points of contact and cross-functional teams, to ensure efficiency in Office daily management of workload and processes, implement solutions for recurring or systemic issues.
- Assisting on managing Office calendar of appointments and meetings ensuring that the schedule is up to date and followed.
- Helping to maintain the on-line CIS/Cyber Security Training and Awareness courses as well as the other relevant CISS/Cyber training and education materials in either hard (e.g. printed leaflets or bulletins) or soft copy.
- Assisting CISSM, by providing constructive suggestions, on improving Office internal procedures and processes, identifying opportunities for process improvements to enhance work efficiency.
- Monitoring and ensuring Office compliance regarding CIS Security rules and regulations, reporting to the CISSM any identified CIS Security loopholes, infringements, vulnerabilities or policy violations.
- 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

- Maintaining a record of all persons authorised to access any part of the common [Infrastructure and Service Delivery Division (IS) provided] NSPA CIS and the extent of their authorisation; controlling that those persons have the appropriate security clearance and need-to-know for the information stored, processed, transmitted by NSPA CIS.
- Processing and coordinating, as required by CISSM, CIS/Cyber Security related forms and requests whether in paper or electronic workflow formats, seeking guidance and support whenever necessary.
- Monitoring and coordinating assignment of Programme Offices and Divisions (POD) CIS Security Inspectors (CISSI) and maintaining up to date CISSI register being published on Goldmine.
- Contributing to daily administrative functions in support of the CISS Office, assisting POD CISSIs in their CISS related duties, as required.
- Monitoring the CISS Office shared mailboxes and Service Desk Tickets, processing and/or distributing/coordinating, as required by CISSM, all incoming requests for CIS Security Office support.
- Preparing and maintaining documentation related to CISS Office front-desk CIS/Cyber security operations and checklists.
- Collecting, categorizing, and tracking relevant information required for various tasks and projects.
- Assisting CISSM and CISS Officers (CISSOs) on arranging meetings and handling related details, such as necessary travel arrangements and/or mission coordination.
- Designing and maintaining well-structured paper and electronic Office filing and collaboration systems, including SharePoint repositories and portals.
- Providing secretarial support, as required, to meetings and boards chaired by the Office.
- Assisting CISSM and CISSOs in preparation of reports, presentations and correspondence as required.
- Monitoring and coordinating proper logging of all CIS security events, incidents, and assistance requests in the designated tracking system.
- Assisting in preparing and providing new users with access to the mandatory security awareness training packages hosted on the Joint Advanced Distributed Learning (JADL) portal.
- Assisting in planning and executing CIS/Cyber awareness and phishing simulation campaigns.
- Assisting CISSM and CISSOs in establishing, reviewing and updating Operating Instructions and Procedures relating to CIS/Cyber Security.
- Controlling and monitoring access to Office sensitive files, SharePoint portal/repositories and file structure, while coordinating their proper maintenance and information management.
- Acquiring, stocking and/or maintaining basic office and CIS Security (e.g. tamperproof seals) or forensic investigations related equipment and supplies as required.
- Coordinating CISS Office webpage content with the Corporate Communications Office's Webmaster.
- In coordination with the NSPA finance, ensuring that financial procedures are followed for the Office allocated budget, prepare the necessary financial documents, follow up on procurement activities to ensure that financial files are correctly processed and maintain records of all Office financial transactions.
- Maintaining the level of knowledge on the subject of CIS/Cyber Security by attending meetings and trainings, as identified and requested by the management.
- Proactively developing skills in areas such as planning and organizing, new technology, and effective communication.

QUALIFICATIONS

General Qualifications

- Complete higher secondary education, equivalent education or relevant professional experience.
- At least 4 years of relevant professional experience, preferably acquired within NATO or another international organization.
- Experience in the administration and delivery of CIS/Cyber Security support services.
- Experience of operational support duties in CIS/Cyber Security domain.
- Sound digital literacy with experience in using office automation systems and software applications, e.g. Microsoft Office Suite (Word, Excel, and PowerPoint).

Specific Qualifications

- Familiarity with scripting or automation tools to streamline repetitive tasks.
- Familiarity with ITSM (IT Service Management) tools like Remedy, Jira, etc. and experience in supporting remote users.
- Proven expertise in managing a large number of end users' requests, handling complex and time-sensitive requests with efficiency, professionalism and solution-oriented mindset.
- Basic knowledge in CIS/Cyber security practices and frameworks.
- Knowledge of NATO CIS/Cyber security regulations and procedures, or other widely recognized CIS/Cyber or Information Security Frameworks, Standards or Best Practices.

LANGUAGE QUALIFICATIONS

- NATO's official languages are English and French. Both languages are important in the work of this post, therefore fluency in one language and working knowledge of the other are essential.

DESIRABLE QUALIFICATIONS

- Foundational knowledge of common methods used to compromise and secure modern CIS infrastructures, as well as an awareness of current cyber threats and the tactics typically employed by hackers.
- Familiarity with the NATO Security Policy and the NSPA Security Regulations.
- Hands-on training on tools related with Information Technology (e.g. SAP, SharePoint) and/or Information Security Management;
- Understanding of the security aspects of system and network administration;
- Familiarity with CIS/Cyber auditing tools (e.g. Splunk) or case management tools, and with remediation/mitigation activities of CIS/Cyber Security incidents.

PERSONAL CHARACTERISTICS

- Ability to prepare and write technical documents and guidelines.
- Strong organizational skills with ability to manage multiple tasks efficiently.
- Strong interpersonal skills to effectively collaborate with office team.
- Ability to maintain confidentiality and handle sensitive information with discretion.
- 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 "sécurité des SIC"

Technicien(ne) adjoint(e) [sécurité des SIC]

Grade : 10:B4

Poste n° : AX-28

Original :	Anglais	|	*Habilitation :*	COSMIC TRÈS SECRET
Date de validation :	4 juin 2026	|	*Lieu d'affectation :*	Capellen, LUX
Validé par :	A. Stoia	|	*Code poste :*	A642

RÉSUMÉ

Responsable envers le/la gestionnaire de la sécurité (SIC et COMSEC), le/la titulaire est chargé(e) de traiter efficacement une large gamme de tâches de soutien opérationnel de nature administrative, relevant des systèmes d'information et de communication (SIC) ou de la cybersécurité, et de nature organisationnelle au niveau du bureau. Il/Elle exerce plus précisément les fonctions suivantes :

RESPONSABILITÉS

Responsabilités générales

- mettre en œuvre, configurer et tenir à jour tous les matériels techniques relevant des SIC et de la cybersécurité, les outils de criminalistique ou d'autres matériels de sécurité du Bureau du/de la responsable en chef de la sécurité, en veillant à leur disponibilité et à la continuité de leur fonctionnement ;
- concevoir, mettre en œuvre et tenir à jour, en coordination avec les services chargés des technologies de l'information et de la communication (TIC) et en appui de ces derniers, des bases de données, des tableaux, des systèmes de suivi et d'autres outils numériques ou flux de travail de processus utilisés au sein du Bureau "sécurité des SIC" ;
- gérer et organiser les documents propres au bureau, ce qui comprend le classement, la numérisation et la tenue de dossiers et de procédures électroniques afin d'assurer l'efficacité du travail requise ;
- aider le/la gestionnaire de la sécurité des SIC à suivre la charge de travail du bureau et à coordonner les congés du personnel du bureau, en veillant à maintenir une couverture nécessaire pour assurer la continuité des processus et des opérations ;
- assurer le soutien des activités liées aux opérations, à la planification et à la coordination du Bureau "sécurité des SIC", conformément aux exigences du/de la gestionnaire de la sécurité des SIC ;
- suivre l'exécution en temps utile des tâches du bureau et coordonner l'adaptation des priorités afin de gérer les demandes urgentes ;
- en liaison avec le/la gestionnaire de la sécurité (SIC et COMSEC) et les responsables, recueillir et analyser les informations relatives aux incidents et violations en matière de SIC ou de cybersécurité afin de mener une analyse des tendances en appui du processus d'amélioration continue ;
- établir et transmettre régulièrement des rapports, des exposés et d'autres documents relatifs à la cybersécurité selon les besoins ;
- assurer la liaison et travailler en collaboration avec des interlocuteurs et des équipes transfonctionnelles afin de veiller à une gestion quotidienne efficace de la charge de travail et des processus au sein du bureau, et mettre en œuvre des solutions aux problèmes récurrents ou systémiques ;
- aider à gérer le calendrier des rendez-vous et des réunions du bureau en veillant à ce que le calendrier soit à jour et respecté ;
- aider à tenir à jour les cours en ligne de formation et de sensibilisation aux SIC et à la cybersécurité ainsi que les autres matériels de formation et supports didactiques relatifs à la sécurité des SIC et à la cybersécurité, soit sur support papier (p. ex. brochures imprimées ou bulletins), soit sur support électronique ;
- aider le/la gestionnaire de la sécurité des SIC, en formulant des suggestions constructives, concernant l'amélioration des procédures et processus internes du bureau, en déterminant les possibilités d'amélioration des processus afin d'accroître l'efficacité du travail ;
- assurer le suivi et le respect de la conformité du bureau en ce qui concerne la réglementation en matière de sécurité des SIC et signaler au/à la gestionnaire de la sécurité des SIC toute faille, infraction, vulnérabilité ou violation de la politique de sécurité des SIC identifiée ;
- 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

- tenir un registre de toutes les personnes autorisées à accéder à toute partie des SIC communs de la NSPA (fournis par la Division "infrastructure et prestation de services"), en précisant l'étendue de cette autorisation ; vérifier que ces personnes sont titulaires de l'habilitation de sécurité nécessaire pour avoir accès aux informations stockées, traitées et transmises par les SIC de la NSPA et qu'elles ont le besoin d'en connaître ;
- traiter et coordonner, conformément aux exigences du/de la gestionnaire de la sécurité des SIC, les formulaires et demandes relatifs aux SIC et à la cybersécurité, tant sur papier que sous format électronique, en demandant des instructions et un soutien lorsque cela est nécessaire ;
- suivre et coordonner l'affectation des inspecteurs de sécurité des SIC des bureaux de programme et divisions (BPD) et tenir à jour le registre des inspecteurs de sécurité des SIC publié sur Goldmine ;
- contribuer à l'exécution des fonctions administratives quotidiennes en appui du Bureau "sécurité des SIC" et aider les inspecteurs de sécurité des SIC des BPD à exercer leurs fonctions liées à la sécurité des SIC, selon les besoins ;
- assurer le suivi des boîtes aux lettres partagées et des tickets du service d'assistance du Bureau "sécurité des SIC" et traiter ou répartir/coordonner, selon les instructions du/de la gestionnaire de la sécurité des SIC, toutes les demandes de soutien reçues par le Bureau "sécurité des SIC" ;
- élaborer et tenir à jour la documentation concernant les opérations et les listes de contrôle du secrétariat du Bureau "sécurité des SIC" pour ce qui concerne les SIC et la cybersécurité ;
- recueillir, classer et contrôler les informations pertinentes nécessaires à divers projets et tâches ;
- aider le/la gestionnaire de la sécurité des SIC et les responsables "sécurité des SIC" à organiser des réunions et à traiter les informations y afférentes, p. ex. les dispositions nécessaires relatives aux déplacements ou la coordination des missions ;
- concevoir et tenir à jour des systèmes collaboratifs et de classement en versions papier et électronique bien structurés, ce qui comprend des bibliothèques et des portails SharePoint ;
- fournir un soutien en matière de secrétariat, selon les besoins, dans le contexte de réunions et de comités présidés par le bureau ;
- aider le/la gestionnaire de la sécurité des SIC et les responsables "sécurité des SIC" à établir des rapports, des exposés et de la correspondance selon les besoins ;
- suivre et coordonner la consignation en bonne et due forme, dans le système de suivi désigné, de tous les événements, incidents et demandes d'assistance liés à la sécurité des SIC ;
- aider à préparer la formation portant sur la sensibilisation obligatoire à la sécurité accessible via le portail du programme interarmées de formation à distance (JADL) et donner aux nouveaux utilisateurs l'accès à ce portail ;
- aider à la planification et à l'exécution de campagnes de sensibilisation aux SIC et à la cybersécurité ainsi que de simulation d'hameçonnage ;
- aider le/la gestionnaire de la sécurité des SIC et les responsables "sécurité des SIC" à établir, revoir et mettre à jour les instructions et procédures d'exploitation relatives aux SIC et à la cybersécurité ;
- contrôler et surveiller l'accès aux fichiers sensibles, aux portails et bibliothèques SharePoint ainsi qu'à la structure des dossiers du bureau, tout en coordonnant leur maintenance et la gestion des informations ;
- acquérir, stocker ou tenir à jour des matériels et des fournitures élémentaires de bureau et liés à la sécurité des SIC (p. ex. indicateurs d'effraction) ou aux enquêtes criminalistiques, selon les besoins ;
- coordonner le contenu de la page web du Bureau "sécurité des SIC" avec le/la webmestre du Bureau de la communication d'entreprise ;
- en coordination avec le service chargé des finances de la NSPA, veiller à ce que les procédures financières soient respectées concernant le budget alloué au bureau, élaborer les documents financiers nécessaires, assurer le suivi des activités relatives aux achats afin que les dossiers financiers soient correctement traités et tenir la comptabilité de toutes les opérations financières du bureau ;
- maintenir le niveau de connaissances en matière de SIC et de cybersécurité en participant à des réunions et à des formations sélectionnées et demandées par la direction ;
- développer de manière proactive des compétences dans des domaines tels que la planification et l'organisation, les nouvelles technologies et la communication efficace.

QUALIFICATIONS

Qualifications générales

- Études secondaires supérieures complètes, formation équivalente ou expérience professionnelle pertinente.
- Au moins quatre années d'expérience professionnelle pertinente, acquise de préférence au sein de l'OTAN ou dans une autre organisation internationale.
- Expérience de l'administration et de la fourniture de services de soutien en matière de SIC et de cybersécurité.
- Expérience des tâches de soutien opérationnel dans le domaine des SIC et de la cybersécurité.
- 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 des outils de script ou d'automatisation permettant de rationaliser des tâches répétitives.
- Connaissance des outils ITSM (gestion des services informatiques) tels que Remedy ou Jira, et expérience du soutien des utilisateurs à distance.
- Compétences confirmées en matière de gestion d'un grand nombre de demandes soumises par les utilisateurs finaux, en faisant preuve d'efficacité, de professionnalisme et d'un sens de la résolution de problèmes dans le traitement de demandes complexes et urgentes.
- Connaissance élémentaire des pratiques et des cadres relatifs aux SIC et à la cybersécurité.
- Connaissance des règles et des procédures de l'OTAN en matière de SIC et de cybersécurité, ou d'autres cadres, normes ou meilleures pratiques largement reconnus en matière de SIC, de cybersécurité ou de sécurité de l'information.

CONNAISSANCES LINGUISTIQUES

- Les langues officielles de l'OTAN sont l'anglais et le français. Les deux langues étant importantes pour le travail effectué à ce poste, il est essentiel d'avoir une bonne maîtrise de l'une et une connaissance pratique de l'autre.

QUALIFICATIONS SOUHAITABLES

- Connaissance fondamentale des méthodes courantes utilisées pour compromettre et sécuriser les infrastructures SIC modernes, et connaissance des cybermenaces actuelles ainsi que des tactiques généralement employées par les pirates informatiques.
- Connaissance de la politique de sécurité de l'OTAN et des règlements de sécurité établis par la NSPA.
- Formation pratique sur les outils liés aux technologies de l'information (p. ex. SAP, SharePoint) ou à la gestion de la sécurité de l'information.
- Compréhension des aspects liés à la sécurité de l'administration des systèmes et des réseaux.
- Connaissance des outils d'audit liés aux SIC et à la cybersécurité (p. ex. Splunk) ou des outils de gestion des dossiers, ainsi que des activités de correction et d'atténuation des incidents liés aux SIC ou à la cybersécurité.

QUALITÉS PERSONNELLES

- Aptitude à élaborer et à rédiger des documents et des directives techniques.
- Solides compétences organisationnelles et aptitude à mener efficacement plusieurs tâches de front.
- Solides compétences en matière de relations interpersonnelles afin de collaborer efficacement avec l'équipe au sein du bureau.
- Aptitude à assurer la confidentialité et à traiter des informations sensibles avec discrétion.
- 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.