



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

Technician (SAC)

Grade: 12:B5

Post No.: AX-30

Original:	English		Clearance:	COSMIC TOP SECRET
Date validated:	13 July 2026		Duty Location:	Pápa, HUN
Validated by:	A. Stoia		Job Code:	A642

SUMMARY

The incumbent reports to the Senior Security Officer (SAC) and is responsible for Site Security/Physical Security and Communication Information Systems Security (CISS) in accordance with NATO, NATO Support and Procurement Organisation (NSPO)/NSPA and the Strategic Airlift Capability Program (SAC Program) prescriptive documents, and providing daily security support to the SAC Program at Pápa, Hungary. More precisely, the incumbent is responsible for executing the following tasks:

RESPONSIBILITIES

General Responsibilities

- Acting as a Site Security/Physical Security Officer and assisting CIS and COMSEC Officer as a Communications Security (COMSEC) specialist.
- Acting as the technical focal point for installation security by planning, implementation and maintenance of physical security systems and force protection measures of the SAC Program, Pápa, Hungary site.
- Supporting the day-to-day operation by monitoring all SAC Program security installations to assure its confidentiality, integrity, availability and effectiveness. Reports discrepancies or technical failures quickly to appropriate personnel for resolution.
- Providing technical expertise supporting the planning, implementation, control, and oversight for all physical security including security system assets and force protection measures of the SAC Program Site.
- Acting as Subject Matter Expert (SME) on new physical security and force protection requirements by supporting NAMP Infrastructure & Facility Mgmt Branch in drafting Statements of Work (SOWs) which fully define the requested services.
- Coordinating with internal stakeholders, external contractors regarding preventive and corrective maintenance, technical inspections, replacements, and technical improvements.
- Assisting in the engagement with Host Nation (HN) authorities for matters involving physical security, force protection and emergency management including COMSEC.
- Assisting the CIS and COMSEC Officer (SAC) with CIS Security including CRYPTO operations, coordination, training and awareness.
- Assisting in the CISS related activities to the CIS Providers, system administrators, users and external contractors, to include functional and technical CISS specifications for projects deriving from business requirements.
- Assisting in CISS inspections of the systems, in order to control and check that classified and NON-Classified electronic information is properly stored, processed, transmitted and safeguarded, whose results are to be forwarded in writing to the Senior Security Officer (SAC) as required.
- Planning and executing relevant CISS and CRYPTO related trainings and awareness for all SAC personnel in cooperation with CIS and COMSEC Officer (SAC).
- Informing the CIS and COMSEC Officer (SAC) of any CISS loopholes, infringements and vulnerabilities or incidents that may come to light, and assisting in local CIS security investigations.

- Assisting with the coordination of security accreditation/reaccreditation tasks for all SAC Program classified and NON-Classified CIS in accordance with NATO policy, supporting directives and Security Accreditation Authority (SAA) requirements and guidance.
- Coordinating with Host Nation (HN) Authorities implementation of physical security and force protection measures in SAC Program installations.
- Coordinating with Host Nation (HN) Authorities preparation and execution of the Emergency and Incident Response exercises.
- Assisting with the execution of local security audits, investigations of security incidents and spot checks.
- 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 with the active leadership and management of the SAC Program site security/physical security, including coordination with HN of the guard force involvement in order to ensure effective delivery of security operations.
- Attending meetings involving SAC Program site security/physical security matters as required.
- Collaborating with NAMP Infrastructure & Facility Mgmt Branch in maintenance visits, repairs, calibrations, and replacements performed by external suppliers or service providers, regarding the security system.
- Conducting or supporting periodic security checks of secure doors, metal grilles, combination locks, perimeter barriers, safes, secure containers, and associated protective measures in order to identify deficiencies, breaches, non-compliance, or conditions affecting physical protection.
- Operating surveillance camera systems and video management platform, including system health checks, retention checks, playback support, and first-line troubleshooting.
- Monitoring intrusion and access control system, coordinating response on system technical failures, tamper events, and equipment failures.
- Supporting the administration of security systems, including, user profile management, system elements checks, and basic technical configuration within delegated authority.
- Providing user guidance and basic familiarization on physical security systems and associated protective measures where required.
- Providing technical support for the provision of the SAC Program Installation security services.
- Assisting with the execution of visitor control and ensures all personnel are subject to appropriate checks before entering the site.
- Assisting with ensuring and verifying that security arrangements for classified meetings are effectively implemented.
- Assisting in the evaluation of security incidents and recommends appropriate action, as required.
- Assisting with the contributions to emergency response planning and to the execution of exercises to validate such plans including development and implementation of NATO Installation Internal Security Plan.
- Assisting in the performance of periodic security inspections and audits and providing the appropriate reports.
- Assisting in the implementation of the site security risk management process.
- Administering SAC Program centrally managed key storing management system.
- Supporting the Facility Management Contractor by advising and first level troubleshooting on Access Control System and Surveillance Camera System.
- Assisting in formulating and maintaining CIS Security Accreditation Documentation Package, including Security Operating Procedures (SecOPs) for all NAM PO CIS, and circulating the SecOPs to system/network administrators and users on a periodic basis.
- Providing security advice to, and maintaining CIS security awareness of system/network administrators and users, in coordination with CISS and COMSEC Officer (SAC).
- Assisting in approving access and maintaining a record of all persons authorized to any part of the NAM PO CIS and the extent of their authorization.

- Assisting in monitoring security-relevant activities, duties and responsibilities of the system administrator, and checking audit information for event / process failure, and unauthorized 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 CIS elements and external mass storage media (EMSM) are being properly controlled and marked with security classification.
- Ensuring computer storage media to be released only contains information authorized for release.
- Monitoring and reporting if 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.
- Monitoring and reporting if CISs / network security relevant information is properly backed up and recovery procedures are in place.
- Verifying the configuration management aspects of changes to security-related hardware, firmware or software and associated documentation.
- Assisting the Senior Security Officer (SAC) in replacing CIS and COMSEC Officer (SAC) 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.
- Minimum 5 years' experience in Site Security/Physical Security and CIS Security in NATO or National Security environment normally acquired as a Technician in the Agency or in a similar organisation.
- Practical experience in technical systems support and management, electronics, telecommunications, or related technical fields, preferable in electronic security systems.
- Knowledge of IT systems with experience in using personal computers and software packages.
- Well-developed communication skills (written, oral and presentation).
- 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, or Communication Security (COMSEC) certified training from NATO or National Security Department or equivalent commercial IT Security training companies.
- Knowledge of NATO Physical Security and Force Protection principles, and their application to the development of an effective NATO Installation Internal Security Plan.
- Knowledge of access control, intrusion detection, surveillance camera system, or related physical security technologies.
- Good knowledge and experience in Risk Analysis and Risk Management methodologies.
- Experience in planning and executing NATO Security Awareness related trainings.
- Proven experience in technical writing and the use of technical data.

LANGUAGE QUALIFICATIONS

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

DESIRABLE QUALIFICATIONS

- Good understanding of the underlying concepts of CIS/IT service management and delivery.
- Experience with integrated security systems, surveillance camera systems, intrusion monitoring platforms, or security management software would be an asset.

- Experience in a NATO, military, governmental, aviation, airfield, or other security-sensitive environment would be an asset.
- Understanding of NATO site security support processes and service delivery concepts would be an advantage.
- Working level knowledge of the Host Nation language (Hungarian).

PERSONAL CHARACTERISTICS

- 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.
- 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 team work toward established objectives.
- Passionate and motivated, equipped with strong communication skills, fostering an environment that encourages community involvement and engagement.
- Ability to empower team work towards established objectives.

ADDITIONAL INFORMATION

- The incumbent will be required to obtain a "Cosmic Top Secret" security clearance.



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

Technicien(ne) [SAC]

Grade : 12:B5

Poste n° : AX-30

Original :	Anglais	Habilitation :	COSMIC TRÈS SECRET
Date de validation :	13 juillet 2026	Lieu d'affectation :	Pápa, HUN
Validé par :	A. Stoia	Code poste :	A642

RÉSUMÉ

Sous la direction du/de la responsable principal(e) de sécurité [capacité de transport aérien stratégique (SAC)], le/la titulaire est chargé(e) de la sécurité du site et de la sécurité physique, ainsi que 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), de la NSPA et du programme SAC. Il/Elle apporte un soutien quotidien en matière de sécurité au programme SAC situé à Pápa, en Hongrie, et exécute plus précisément les tâches suivantes :

RESPONSABILITÉS

Responsabilités générales

- faire fonction de responsable de la sécurité du site et de la sécurité physique et, en qualité de spécialiste de la sécurité des communications (COMSEC), aider le/la responsable SIC et COMSEC ;
- faire fonction de point de contact technique pour la sécurité des installations, en assurant la planification, la mise en œuvre et la maintenance des systèmes de sécurité physique et des mesures de protection des forces du programme SAC situé à Pápa, en Hongrie ;
- soutenir l'activité quotidienne en assurant le suivi de toutes les installations de sécurité du programme SAC afin d'assurer leur confidentialité, leur intégrité, leur disponibilité et leur efficacité ; signaler rapidement les anomalies ou les défaillances techniques au personnel concerné afin de les résoudre ;
- mettre à disposition des compétences techniques en appui de la planification, de la mise en œuvre, du contrôle et de la supervision de l'ensemble de la sécurité physique, ce qui comprend le matériel de système de sécurité et les mesures de protection des forces du site du programme SAC ;
- faire fonction d'expert technique concernant les nouvelles exigences en matière de sécurité physique et de protection des forces en apportant un soutien à la Branche "infrastructures et gestion des installations" du programme OTAN de gestion du transport aérien (NAM) dans l'élaboration des cahiers des charges qui définissent complètement les services demandés ;
- coordonner avec les parties prenantes internes et les titulaires de marché externes la maintenance préventive et corrective, les inspections techniques, les remplacements et les améliorations techniques ;
- apporter une aide dans le contexte de la coopération avec les autorités du pays hôte pour les questions relatives à la sécurité physique, à la protection des forces et à la gestion des urgences, ce qui comprend la COMSEC ;
- aider le/la responsable SIC et COMSEC (SAC) concernant la sécurité des SIC, ce qui comprend l'exploitation, la coordination, la formation et le maintien des connaissances en matière de systèmes cryptographiques ;
- aider les fournisseurs des SIC, les administrateurs de systèmes, les utilisateurs et les titulaires de marché externes en ce qui concerne les activités relatives à la sécurité des SIC, ce qui comprend les spécifications fonctionnelles et techniques relatives à la sécurité des SIC au titre de projets découlant de besoins opérationnels ;
- participer aux inspections de sécurité des SIC, de manière à contrôler et vérifier que les informations électroniques classifiées et non classifiées sont correctement stockées, traitées, transmises et sauvegardées, inspections dont les résultats doivent être communiqués par écrit au/à la responsable principal(e) de sécurité (SAC) selon les besoins ;
- planifier et dispenser les formations et les ateliers de sensibilisation pertinents en matière de sécurité des SIC et de cryptographie pour l'ensemble du personnel de la SAC, en coopération avec le/la responsable SIC et COMSEC (SAC) ;
- informer le/la responsable SIC et COMSEC (SAC) de toute faille, violation ou vulnérabilité relatives à la sécurité des SIC et de tout incident qui se produirait en la matière, et participer aux enquêtes locales de sécurité des SIC ;

- aider à coordonner des tâches d'homologation ou de renouvellement d'homologation de sécurité concernant tous les SIC classifiés et non classifiés du programme SAC, conformément à la politique générale de l'OTAN, aux directives complémentaires et aux exigences et orientations des autorités d'homologation de sécurité ;
- coordonner avec les autorités du pays hôte la mise en œuvre de la sécurité physique et des mesures de protection des forces au sein des installations du programme SAC ;
- coordonner avec les autorités du pays hôte la préparation et la réalisation des exercices d'intervention d'urgence et de réponse aux incidents ;
- participer à la réalisation des audits locaux de sécurité, des enquêtes portant sur les incidents de sécurité et des contrôles inopinés ;
- 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 assurer le leadership actif et la gestion de la sécurité du site et de la sécurité physique du programme SAC, ce qui comprend la coordination, avec le pays hôte, de l'intervention du service des gardes pour veiller au déroulement efficace des opérations de sécurité ;
- participer aux réunions portant sur des questions de sécurité du site et de sécurité physique du programme SAC, selon les besoins ;
- collaborer avec la Branche "infrastructures et gestion des installations" du programme NAM lors des visites de maintenance, des réparations, des calibrages et des remplacements effectués par des fournisseurs ou des prestataires de services externes sur le système de sécurité ;
- mener ou aider à la réalisation de vérifications de sécurité périodiques concernant les portes sécurisées, les grillages métalliques, les serrures à combinaison, les clôtures périphériques, les coffres-forts, les meubles sécurisés et les mesures de protection connexes, afin de détecter les insuffisances, les manquements, les cas de non-conformités ou les conditions altérant la protection physique ;
- exploiter les systèmes de vidéosurveillance et la plate-forme de gestion des vidéos, ce qui comprend les contrôles d'intégrité des systèmes, les vérifications relatives à la durée de conservation des enregistrements, l'assistance à la lecture de ces derniers et le dépannage de première ligne ;
- vérifier le système de détection des intrusions et de contrôle des accès, coordonner les réponses en cas de défaillance technique du système, d'actes de sabotage ou de panne matérielle ;
- soutenir l'administration des systèmes de sécurité, ce qui comprend la gestion des profils d'utilisateurs, les vérifications des éléments de système et la configuration technique de base dans les limites de sa délégation de pouvoir ;
- donner aux utilisateurs des orientations et des connaissances élémentaires sur les systèmes de sécurité physique et les mesures de protection connexes en fonction des besoins ;
- fournir un soutien technique dans le domaine des services liés à la sécurité des installations du programme SAC ;
- aider à l'exécution du contrôle des visiteurs et veiller à ce que tous les membres du personnel fassent l'objet de contrôles appropriés avant d'entrer sur le site ;
- aider à veiller à ce que les mesures de sécurité afférentes aux réunions classifiées soient effectivement appliquées, et procéder à des vérifications ;
- aider à évaluer les incidents de sécurité et recommander les dispositions nécessaires selon les besoins ;
- aider à contribuer à la planification des interventions en cas d'urgence et à la réalisation d'exercices permettant de valider ces plans, ce qui comprend l'élaboration et la mise en œuvre du plan de sécurité intérieure des installations de l'OTAN ;
- aider à procéder à des inspections et à des audits de sécurité périodiques, et fournir les rapports correspondants ;
- participer à la mise en œuvre du processus de gestion des risques de sécurité du site ;
- administrer le système de gestion du stockage des clés du programme SAC, qui est géré de façon centralisée ;
- aider le titulaire du marché portant sur la gestion des installations en le conseillant et en assurant le dépannage de premier niveau du système de contrôle d'accès et du système de vidéosurveillance ;
- aider à rédiger et à tenir à jour l'ensemble de la documentation portant sur les homologations de sécurité des SIC, ce qui comprend les procédures d'exploitation de sécurité (SecOPs) pour l'ensemble des SIC du Bureau de programme NAM, et communiquer ces SecOPs périodiquement aux administrateurs et aux utilisateurs des systèmes et des réseaux ;
- donner des conseils de sécurité aux administrateurs et aux utilisateurs des systèmes et des réseaux, et maintenir leur niveau d'information en matière de sécurité des SIC, en coordination avec le/la responsable SIC et COMSEC (SAC) ;
- aider à approuver les accès et à tenir un registre de toutes les personnes autorisées à accéder à toute partie des SIC du Bureau de programme NAM, en précisant l'étendue de cette autorisation ;

- aider à 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 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 supports de stockage de données devant être fournis ne contiennent que des informations dont la divulgation est autorisée ;
- contrôler si les titulaires de marché ou autres organismes destinataires de supports de stockage de données classifiés ont en place des dispositions de sécurité et s'ils ont le besoin d'en connaître, conformément aux exigences de la politique de sécurité de l'OTAN et de ses directives complémentaires, et en rendre compte ;
- vérifier si les informations ayant une incidence sur la sécurité des SIC et des réseaux sont correctement sauvegardées et si des procédures de récupération sont en place, et en rendre compte ;
- vérifier les aspects relatifs à la gestion de la configuration des modifications des matériels, des micrologiciels ou des logiciels liés à la sécurité, ainsi que de la documentation connexe ;
- aider le/la responsable principal(e) de sécurité (SAC) à remplacer le/la responsable SIC et COMSEC (SAC) en son 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 appropriée et pertinente.
- Au moins cinq années d'expérience de la sécurité de site, de la sécurité physique et de la sécurité des SIC dans un environnement de sécurité OTAN ou national, normalement acquise en qualité de technicien(ne) au sein de l'Agence ou d'un organisme similaire.
- Expérience pratique du soutien et de la gestion de systèmes techniques, de l'électronique, des télécommunications ou de domaines techniques connexes, de préférence en lien avec les systèmes de sécurité électroniques.
- Connaissance des systèmes informatiques assortie d'une expérience de l'utilisation d'ordinateurs personnels et de progiciels.
- Compétences bien établies en matière de communication (par écrit, à l'oral et lors d'exposés).
- 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, 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 l'OTAN relatifs à la sécurité physique et à la protection des forces, ainsi que de leur application en vue de l'élaboration d'un plan de sécurité intérieure efficace des installations OTAN.
- Connaissance des technologies de contrôle d'accès, de détection des intrusions, des systèmes de vidéosurveillance ou de toute technologie de sécurité physique connexe.
- Bonne connaissance et expérience des méthodes d'analyse et de gestion de risques.
- Expérience de la planification et de la dispense de formations de sensibilisation à la sécurité de l'OTAN.
- Expérience démontrée en matière de rédaction de textes techniques et d'exploitation de données 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

- Bonne compréhension des concepts sur lesquels s'appuient la gestion et la fourniture de services SIC ou informatiques.
- Une expérience des systèmes de sécurité intégrés, des systèmes de vidéosurveillance, des plates-formes de détection d'intrusions ou des logiciels de gestion de la sécurité constituerait un atout.

- Une expérience dans un environnement OTAN, militaire ou gouvernemental, dans le milieu de l'aviation ou dans un aéroport, ou dans tout autre environnement sensible en matière de sécurité, constituerait un atout.
- La compréhension des processus de soutien à la sécurité des sites de l'OTAN et des concepts de fourniture de services constituerait un atout.
- Connaissance pratique de la langue du pays hôte, le hongrois.

QUALITÉS PERSONNELLES

- 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.
- 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.
- Capacité à valoriser le travail d'équipe dans le but de réaliser les objectifs fixés.

INFORMATIONS COMPLÉMENTAIRES

- Il sera attendu du/de la titulaire qu'il/elle obtienne une habilitation de sécurité "COSMIC TRÈS SECRET".