



INITIAL ALLIANCE FUTURE SURVEILLANCE AND CONTROL (iAFSC) PROGRAMME OFFICE

Senior Technical Officer (Information Security)

Grade: 17:A3

Post No.: QI-11

Original:	English		Clearance:	NATO Secret
Date validated:	20 August 2026		Duty Location:	Capellen, LUX
Validated by:	J. Schimek		Job Code:	A622

SUMMARY

The incumbent reports to the Chief of Branch and is responsible for performing all functions related to the information security and security accreditation of the initial Alliance Surveillance and Control (iAFSC) System. More precisely, the incumbent is responsible for performing the following functions:

RESPONSIBILITIES

General Responsibilities

- Assisting the lead engineer in developing and implementing a robust Communications and Information Systems (CIS) Information Assurance strategy for activities related to the iAFSC Programme.
- Managing the CIS Information assurance technical and engineering aspects of the iAFSC system including system and sub system qualification, accreditation and security management.
- Assisting in preparing and coordinating the annual workload forecasts.
- Contributing to all information security aspects of CIS of the iAFSC System.
- Assuming responsibility for the execution of assigned tasks in the area of iAFSC Programme Information Assurance and Cyber Defence.
- Ensuring that all Information Security (InfoSec) requirements are implemented by contractors.
- Performing security audits in contractor's premises to ensure that contractual requirements related to the protection, handling and integrity of the information are satisfied.
- Ensuring that selected implementation is consistent and compliant with other NATO and national requirements; to this extent interacting very closely with NATO and allied security agencies representing NSPA position.
- Defining, with the support of the relevant Subject Matter Expert (SME), hardware and software security requirements for the overall project and subprojects.
- Providing security assessment and impact analysis on engineering change proposals affecting the iAFSC System, including its interfaces with external systems and networks.
- Assisting the lead engineer in the definition of security requirements affecting the design and implementation of system modifications.
- Ensuring compliance with infrastructure requirements related with Information Assurance.
- Maintaining awareness in their respective domain with regard to new technologies, and identification of new types of security threats and vulnerabilities.
- Assuming responsibility for the maintenance of the Security Accreditation of the iAFSC.
- Identifying schedule, cost and performance risks in their area of responsibility, evaluating the risk, assessing mitigation plans and monitoring implementation activities.

- Producing, updating and maintaining the iAFSC System Management Security Instruction.
- Performing Travel on Duty (TDY) as required, in accordance with the NATO Civilian Personnel Regulations (NCPR).
- 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

- Development and monitoring the iAFSC System security accreditation documentation and certification.
- Providing timely expert advice and support to senior management and Agency staff in the area of Information Assurance and Cyber Defence during the life cycle of the iAFSC Programme.
- Liaising with external security authorities to include the NATO Office of Security (NOS), NATO Communications and Information Agency (NCIA), Supreme Headquarters Allied Powers Europe (SHAPE), the Host Nation Security Services, Security Officers of the iAFSC nations and security officers of the contracting firms, on all CIS Information Security matters.
- Acting as SME and advisor on technical matters related to IA on the iAFSC System.
- Overseeing the iAFSC information systems development and interoperability.
- Assisting the lead engineer and Airworthiness engineer developing the information security approach for Type Certification with the German Military Aviation Authority (German)
- Developing necessary directives and plans for the implementation of IA policies for the iAFSC system.
- Conducting inspections, evaluations to confirm Industry's accreditation of systems and facilities related with iAFSC System.
- Conducting Security Risk Assessments and providing risk management recommendations.
- Advising on the technical requirements for all internal iAFSC security-based requirements and drafting Operational Requirements on all cryptographic matters.
- Assuming responsibility for all aspects related to the security accreditation of the iAFSC Logistics Information System.
- Cooperating with Verification and Certification Engineers for setting up demonstration and/or test plans and for evaluating and resolving of Information Assurance issues that are discovered during the demonstration and testing.
- Identifying risks in their area of responsibility, assessing risks identified by directed staff, assessing risk mitigation activities.
- Representing the iAFSC Engineering team up to their level of authority during interactions with governmental entities, NATO entities and the industry.

QUALIFICATIONS

General Qualifications

- University degree in Cyber Security, Communications Engineering, Communication and Information Systems Engineering, Computer Science or a closely related field, equivalent education, or relevant professional experience.
- Minimum eight years' experience, at management level, in several fields of the following: Protective security and counter-intelligence (including Physical Protective Measures, Security of Information, IA and Security Education); Wide Area Network (WAN) and Local Area Network (LAN) planning and operations, development and management of command-and-control information systems (CCIS) and management information systems (MIS), Crypto management and equipment.
- Experience in leading complex multi-disciplined projects.
- Ability to facilitate/present persuasively and negotiate effectively to achieve desired outcomes.
- Ability to develop resourceful and effective solutions to problems (including personnel), focus on team performance goals and track metrics to measure performance improvements.

- High degree of flexibility and agility to adapt to a changing environment and to lead change implementation.
- Sound digital literacy with experience in using office automation systems and software applications, e.g. Microsoft Office Suite (Word, Excel, and PowerPoint).

Specific Qualifications

- Qualified and experienced in leading, chairing and organising multi-national committees, Working Groups (WGs) and conferences.
- Experience in and up-to-date knowledge of security functions supporting the military operational deployment of Airborne Early warning and control or C4ISR military systems in both static and deployable environments.
- Familiarity with satellite communications technologies and operations.

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

- Good knowledge of the NATO Information Security and Cyber Defence policies and regulations.
- Advanced security-related certification (i.e. CISSP, Security+).
- PRINCE2® certification.

PERSONAL CHARACTERISTICS

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

ADDITIONAL INFORMATION

- N/A



BUREAU DE PROGRAMME "VOLET INITIAL DE LA FUTURE CAPACITÉ DE SURVEILLANCE ET DE CONTRÔLE DE L'ALLIANCE (iAFSC)"

Responsable technique principal(e) [sécurité de l'information]

Grade : 17:A3

Poste n° : QI-11

Original :	Anglais	Habilitation :	NATO SECRET
Date de validation :	20 août 2026	Lieu d'affectation :	Capellen, LUX
Validé par :	J. Schimek	Code poste :	A622

RÉSUMÉ

Responsable envers le/la chef de branche, le/la titulaire exerce toutes les fonctions afférentes à la sécurité de l'information et à l'homologation de sécurité du système "volet initial de la capacité de surveillance et de contrôle de l'Alliance (iAFSC)". Il/Elle exerce plus précisément les fonctions suivantes :

RESPONSABILITÉS

Responsabilités générales

- aider l'ingénieur(e) principal(e) à développer et à mettre en œuvre une stratégie solide en matière d'assurance de l'information pour les systèmes d'information et de communication (SIC) des activités relevant du programme iAFSC ;
- gérer les aspects techniques et d'ingénierie liés à l'assurance de l'information des SIC du système iAFSC, notamment la qualification, l'homologation et la gestion de la sécurité du système et des sous-systèmes ;
- aider à établir et à coordonner les prévisions annuelles de charge de travail ;
- contribuer à tous les aspects de la sécurité des SIC du système iAFSC ;
- assumer la responsabilité de l'exécution des tâches qui lui sont confiées dans le domaine de l'assurance de l'information et de la cyberdéfense du programme iAFSC ;
- veiller à ce que tous les besoins en matière de sécurité des informations soient mis en œuvre par les titulaires de marché ;
- procéder à des audits de sécurité dans les locaux des titulaires de marché afin de s'assurer que les exigences contractuelles relatives à la protection, à la manipulation et à l'intégrité des informations soient satisfaites ;
- veiller à ce que la mise en œuvre retenue soit conforme et compatible avec d'autres exigences OTAN et nationales ; à cet égard, interagir très étroitement avec les agences de sécurité de l'OTAN et des pays de l'Alliance en présentant la position de la NSPA ;
- définir, avec le soutien de l'expert(e) sectoriel(le) concerné(e), les besoins en matière de sécurité des matériels et des logiciels pour l'ensemble du projet et des sous-projets ;
- fournir des évaluations de sécurité et des études d'impact concernant les propositions de modification technique touchant le système iAFSC, notamment ses interfaces avec des systèmes et des réseaux externes ;
- aider l'ingénieur(e) principal(e) à définir les besoins de sécurité ayant une incidence sur l'élaboration et la mise en œuvre des modifications du système ;
- veiller au respect des exigences en matière d'infrastructures pour ce qui concerne l'assurance de l'information ;
- se tenir au courant des nouvelles technologies dans son domaine de compétence et suivre l'apparition de nouveaux types de menaces et de vulnérabilités pour la sécurité ;
- assumer la responsabilité de la tenue à jour de l'homologation de sécurité du système iAFSC ;
- identifier et évaluer, dans son domaine de responsabilité, les risques ayant une incidence sur les calendriers, les coûts et les performances, évaluer les plans d'atténuation des risques et suivre les activités liées à leur mise en œuvre ;

- élaborer, actualiser et assurer la tenue de l'instruction de sécurité relative à la gestion du système iAFSC ;
- effectuer des déplacements de service selon les besoins conformément au Règlement du personnel civil de l'OTAN ;
- 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

- élaborer et suivre les documents relatifs à l'homologation et à la certification de sécurité du système iAFSC ;
- fournir en temps utile des avis de spécialiste et un soutien à l'encadrement supérieur et au personnel de l'Agence dans le domaine de l'assurance de l'information et de la cyberdéfense au cours du cycle de vie du programme iAFSC ;
- assurer la liaison avec les autorités de sécurité extérieures, à savoir le Bureau de sécurité de l'OTAN (NOS), l'Agence OTAN d'information et de communication (NCIA), le Grand quartier général des puissances alliées en Europe (SHAPE), les services de sécurité du pays hôte, les officiers de sécurité des pays du système iAFSC et les responsables de la sécurité des entreprises sous contrat, concernant toutes les questions liées à la contre-ingérence ;
- jouer le rôle d'expert(e) sectoriel(le) et de conseiller(-ère) reconnu(e) pour les questions techniques liées à l'assurance de l'information dans le cadre du système iAFSC ;
- assurer la supervision de la mise au point et de l'interopérabilité des systèmes d'information du système iAFSC ;
- aider l'ingénieur(e) principal(e) et l'ingénieur(e) "navigabilité" à élaborer la démarche de certification de type avec l'autorité allemande de l'aviation militaire ;
- élaborer les directives et les plans nécessaires à la mise en œuvre des politiques générales en matière d'assurance de l'information pour le système central iAFSC ;
- mener des inspections et des évaluations afin de confirmer l'homologation par l'industrie de systèmes et de moyens liés au système central iAFSC ;
- réaliser des évaluations de risques de sécurité et formuler des recommandations en matière de management du risque ;
- donner des avis sur les exigences techniques concernant tous les besoins internes de sécurité de l'iAFSC et rédiger les énoncés de besoins opérationnels concernant toutes les questions cryptographiques ;
- assumer la responsabilité de tous les aspects liés à l'homologation de sécurité du système d'information logistique de l'iAFSC ;
- coopérer avec les ingénieurs chargés de la vérification et de l'homologation pour mettre en place des plans de démonstration et/ou d'essais ainsi que pour évaluer et résoudre des problèmes d'assurance de l'information décelés lors des démonstrations et essais ;
- identifier les risques dans son domaine de responsabilité, évaluer les risques constatés par les membres du personnel relevant de son autorité et évaluer les activités d'atténuation des risques ;
- représenter l'équipe d'ingénieurs du système iAFSC à hauteur de son niveau de pouvoir lors d'interactions avec les services officiels, les organismes de l'OTAN et l'industrie.

QUALIFICATIONS

Qualifications générales

- Diplôme d'études supérieures en cybersécurité, en ingénierie des télécommunications, en ingénierie des systèmes d'information et de communication, en informatique ou dans un domaine étroitement lié, formation équivalente ou expérience professionnelle pertinente.
- Une expérience d'au moins huit années, acquise au niveau de l'encadrement, dans plusieurs domaines parmi les suivants : sécurité préventive et contre-ingérence (notamment les mesures de protection physique, la sécurité de l'information, l'assurance de l'information et la formation à la sécurité) ; planification et exploitation de réseaux à grande distance (WAN) et de réseaux locaux (LAN), mise au point et gestion

de systèmes d'information de commandement et de contrôle (CCIS) et de systèmes d'information de gestion (MIS), gestion et matériels cryptographiques.

- Expérience de la direction de projets multidisciplinaires complexes.
- Aptitude à animer/exposer avec conviction et à mener des négociations efficaces permettant d'atteindre les résultats souhaités.
- Aptitude à mettre au point des solutions ingénieuses et efficaces aux problèmes (notamment en ce qui concerne le personnel), à se concentrer sur les résultats visés de l'équipe et à suivre les indicateurs afin de mesurer l'évolution des prestations.
- Très grande souplesse et capacité à s'adapter à un environnement changeant et à piloter la mise en œuvre du changement.
- 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

- Qualification et expérience en matière de direction, de présidence et d'organisation de comités, de groupes de travail et de conférences multinationaux.
- Expérience et connaissances à jour des fonctions liées à la sécurité en appui du déploiement opérationnel militaire de systèmes aéroportés de détection lointaine et de contrôle et de systèmes militaires de commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance dans des contextes statiques et de déploiement.
- Connaissance des technologies de télécommunications par satellite et de leur exploitation.

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 connaissance de la politique générale et des règlements de l'OTAN en matière de sécurité de l'information et de cyberdéfense.
- Certification avancée dans le domaine de la sécurité [c.-à-d. CISSP (professionnel certifié de la sécurité des systèmes d'information), Security +].
- Certification PRINCE2®.

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

INFORMATIONS COMPLÉMENTAIRES

- S.O.