NATO
NORTH ATLANTIC TREATY ORGANIZATION
INTERNATIONAL STAFF

OTAN
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
SECRÉTARIAT INTERNATIONAL

VACANCY NOTIFICATION/ NOTIFICATION DE LA VACANCE DU POSTE

Officer, Defensive Cyberspace Operations-241436

Primary Location Belgium-Brussels
NATO Body NATO International Staff (NATO IS)
Schedule Full-time
Application Deadline 03-Nov-2024, 11:59:00 PM
Salary (Pay Basis) 7,540.44Euro (EUR) Monthly
Grade NATO Grade G17

Description

"Pending Budget approval"

1. SUMMARY

The NATO Chief Information Officer (CIO) function brings Information and Communications Technology (ICT) coherence across NATO Enterprise's civil and military bodies. The NATO CIO is empowered to realize the Allies' vision for the NATO Enterprise, is accountable to the Secretary General, and is responsible for the development of Enterprise directives and advice on the acquisition and use of information technologies and services. The NATO CIO provides Enterprise oversight on cybersecurity issues and, in close coordination with all relevant NATO civil and military bodies, works towards the continual improvement of the cyber hygiene and cybersecurity posture in the NATO Enterprise.

The Office of the NATO CIO (OCIO) is an integrated staff organisation comprised of International Staff (IS) and International Military Staff (IMS) members. The OCIO supports the planning, coordination and execution of Defensive Cyberspace Operations (DCO) in NATO networks, as one of the leading members of the DCO Planning and Coordination Cell (DPCC). The DPCC is composed of representatives from NATO Cyberspace Operations Centre (CyOC), Joint Intelligence and Security Division (JISD), NATO Communications and Information Agency (NCIA) and OCIO.

The Enterprise Security Branch (ESec) maintains Enterprise oversight on cybersecurity and enables awareness on specific risks, processes and incidents. It supports the NATO CIO in managing cybersecurity risks and incidents at Enterprise level, advises and supports the decision-making process for identifying the Enterprise risk appetite and risk tolerance. The Branch executes functions deriving from the Enterprise risk owner and top-level incident manager roles for cybersecurity, coordinating incident response, business impact analysis, risk mitigation, mid- to long- term measures and lessons-identified. The Branch also maintains relations with key Enterprise military and civilian stakeholders at strategic, operational, tactical and technical levels.

The Security Processes Section (SPS) is responsible for ensuring correct support and representation in its role of Enterprise incident manager in front of multiple NATO relevant cyberspace stakeholders. The section is also responsible to provide liaison to network security, threats analysis and advanced technical operations in support of the defence of NATO Enterprise networks, services and capabilities.

The incumbent is responsible for the coordination of the work of the DPCC, ensuring appropriate and timely communication and cooperation amongst the relevant NATO Enterprise stakeholders (CyOC, JISD, and NCIA). The incumbent is responsible for managing the complete lifecycle of DCO, including the proposal, planning, conduct, assessment and follow-up phases defined in the DCO process. The incumbent supports the DPCC meetings, facilitating discussions, and contributing to the decision making process. The incumbent leads and develops DCO activities in close coordination with the cyber incident management and cyber risk management processes.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- possess a university degree, or an equivalent level of qualification, from an institute of recognised standing, preferably in information and communications technology or a cybersecurity related discipline;
- have at least 3 years of experience in cybersecurity, preferably in a large organisation;
- have experience in managing the development and implementation of cybersecurity capabilities and related security processes;
- possess experience in developing and implementing processes and procedures in support of advanced technical operations;
- have good knowledge and experience in planning, coordinating and executing advanced technical operations, including threat hunting activities adversary emulation and deception technologies;
- have good knowledge in cyber incident management and cyber risk management best practices and processes;
- be familiar with network and infrastructure security principles governing cybersecurity;
- have good knowledge of the principles, policy and procedures governing cybersecurity, preferably in military and/or defence organisations;
- be able to prepare and deliver clear and concise presentations and reports to both technical and non-technical audiences;
- demonstrate strong stakeholder management;
- possess excellent analytical, problem solving, and verbal and written communication skills;
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; I ("Beginner") in the other;
- be flexible and willing to work outside of normal office hours, during incident management activities, and able and willing to travel when required.

DESIRABLE

The following are considered an advantage:

- cybersecurity certifications such as CISSP, CCSP, CISM or equivalent post-graduate degree in cybersecurity;
- experience with NATO's cybersecurity environment, specifically in the CIS security field and related functions;
- experience working on complex projects and coordinating multiple stakeholders in separate locations;
- experience working within a complex, international organisation;
- understanding of NATO's organisation, its security policy and supporting directives;
- good understanding of current and emerging ICT technologies and how enterprises are employing them to drive digital business.

3. MAIN ACCOUNTABILITIES

Policy Development

Contribute to the development of policy, directives, and guidance documents in the OCIO areas of responsibility as per the incumbent's area of expertise. Provide advice to the Section Head on DCO activities, processes and procedures. Provide advice and guidance on DCO to NATO Nations, NATO civil and military bodies, partner nations and international organisations. Develop high-level strategic documents and advice to support the Enterprise DCO processes and procedures.

Expertise Development

Propose, plan, conduct, assess and follow-up DCO activities in close coordination with the cyber incident management and cyber risk management processes and the relevant NATO Enterprise stakeholders. Coordinate DCO activities with Allies and industry and develop a surge capacity framework in the context of DCO. Identify, develop and test new capabilities in support of DCO. Keep abreast with the latest technology developments in the incumbent's area of responsibilities and provide appropriate advice. Propose updates and improvements based on lessons identified from real life experience and from exercises.

Project Management

Support the definition of the section projects plan according to the OCIO role(s) in project management processes used in the NATO Enterprise. Identify main decision-makers and other stakeholders relevant for the project success. Participate and contribute to project management boards as required. Maintain full understanding of project and programme plans, identify and monitor project implementation risks, provide expertise and leadership in the resolution of exceptions and issues. Establish and maintain a network of relations with key project leaders in the NATO Enterprise, with a specific focus on ICT and Cybersecurity projects.

Stakeholder Management

Establish and maintain a network of relations with key experts in the NATO Enterprise, with a specific focus on Enterprise-wide security. Develop close cooperation and working relationships with the relevant NATO stakeholders involved in the lifecycle of Enterprise security processes and practices, with a focus on DCO. Provide Cybersecurity advice and guidance to NATO bodies, nations, civilian and military stakeholders on the planning, conduct and assessment of DCO activities. Be comfortable in chairing, supporting and interacting with executive/senior-level boards and committees.

Knowledge Management

Draft background briefs, progress reports, prepare presentations, and other items for high-level meetings. Contribute to the information sharing with the relevant NATO bodies and stakeholders (e.g. NATO Cyber Risk management Group (CRMG), the NATO Board of CISOA (BCISOA)) that may contribute and support DCO activities. On the basis of briefings, discussions and investigations, provide advice on evolving security programmes in NATO nations, NATO civilian and military bodies, and non-NATO entities. Identify advanced technical operations capabilities existing within the NATO Enterprise, but also new ones to be developed in support of DCO.

Financial Management

Manage a predetermined budget for assigned projects.

Planning and Execution

Plan, conduct, assess and follow-up DCO activities on NATO networks, in close coordination with the relevant Enterprise stakeholders, bodies and groups. Coordinate and develop the processes and procedures required to support the different phases of the DCO lifecycle.

4. INTERRELATIONSHIPS

The incumbent reports to the Head, Security Processes Section. The incumbent works in close cooperation with the OCIO members of staff as well with experts of the various NATO Entities.

Direct reports: N/A

Indirect reports: N/A

5. COMPETENCIES

The incumbent must demonstrate:

- Analytical Thinking: Sees multiple relationships.
- Flexibility: Adapts to unforeseen situations.
- Impact and Influence: Takes multiple actions to persuade.
- Initiative: Is decisive in a time-sensitive situation.

- Organizational Awareness: Understands organisational climate and culture.
- Teamwork: Cooperates.

6. CONTRACT

Contract to be offered to the successful applicant (if non-seconded): Definite duration contract of three years; possibility of renewal for up to three years, during which the incumbent may apply for conversion to an indefinite duration contract.

Contract clause applicable:

In accordance with the contract policy, this is a post in which turnover is desirable for political reasons in order to be able to accommodate the Organisation's need to carry out its tasks as mandated by the Nations in a changing environment, for example by maintaining the flexibility necessary to shape the Organisation's skills profile, and to ensure appropriate international diversity.

The maximum period of service foreseen in this post is 6 years. The successful applicant will be offered a 3-year definite duration contract, which may be renewed for a further period of up to 3 years. However, according to the procedure described in the contract policy the incumbent may apply for conversion to an indefinite contract during the period of renewal and no later than one year before the end of contract.

If the successful applicant is seconded from the national administration of one of NATO's member States, a 3-year definite duration contract will be offered, which may be renewed for a further period of up to 3 years subject also to the agreement of the national authority concerned. The maximum period of service in the post as a seconded staff member is six years.

Serving staff will be offered a contract in accordance with the NATO Civilian Personnel Régulations.

7. USEFUL INFORMATION REGARDING APPLICATION AND RECRUITMENT PROCESS

Please note that we can only accept applications from nationals of NATO member countries. Applications must be submitted using e-recruitment system, as applicable:

- For NATO civilian staff members only: please apply via the internal recruitment portal (link);
- For all other applications: www.nato.int/recruitment

Before you apply to any position, we encourage you to click here and watch our video providing 6 tips to prepare you for your application and recruitment process.

Do you have questions on the application process in the system and not sure how to proceed? Click here for a video containing the information you need to successfully submit your application on time.

More information about the recruitment process and conditions of employment, can be found at our website (http://www.nato.int/cps/en/natolive/recruit-hq-e.htm)

Appointment will be subject to receipt of a **security clearance** (provided by the national Authorities of the selected candidate), approval of the candidate's **medical file** by the NATO Medical Adviser, verification of your study(ies) and work experience, and the successful completion of the **accreditation** and notification process by the relevant authorities.

NATO will not accept any phase of the recruitment and selection prepared, in whole or in part, by means of generative artificial-intelligence (AI) tools, including and without limitation to chatbots, such as Chat Generative Pre-trained Transformer (Chat GPT), or other language generating tools. NATO reserves the right to screen applications to identify the use of such tools. All applications prepared, in whole or in part, by means of such generative or creative AI applications may be rejected without further consideration at NATO's sole discretion, and NATO reserves the right to take further steps in such cases as appropriate.

8. ADDITIONAL INFORMATION

NATO is committed to diversity and inclusion, and strives to provide equal access to employment, advancement and retention, independent of gender, age, nationality, ethnic origin, religion or belief, cultural background, sexual orientation, and disability. NATO welcomes applications of nationals from all member Nations, and strongly encourages women to apply.

Building Integrity is a key element of NATO's core tasks. As an employer, NATO values commitment to the principles of integrity, transparency and accountability in accordance with international norms and practices established for the defence and related security sector. Selected candidates are expected to be role models of integrity, and to promote good governance through ongoing efforts in their work.

Due to the broad interest in NATO and the large number of potential candidates, telephone or e-mail enquiries cannot be dealt with.

Applicants who are not successful in this competition may be offered an appointment to another post of a similar nature, albeit at the same or a lower grade, provided they meet the necessary requirements.

The nature of this position may require the staff member at times to be called upon to travel for work and/or to work outside normal office hours.

The organization offers several work-life policies including Teleworking and Flexible Working arrangements (Flexitime) subject to business requirements.

Please note that the International Staff at NATO Headquarters in Brussels, Belgium is a non-smoking environment.

For information about the NATO Single Salary Scale (Grading, Allowances, etc.) please visit our website. Detailed data is available under the Salary and Benefits tab.

Administratrice/Administrateur (opérations cybernétiques défensives)-241436

Emplacement principal : Belgique-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 03-nov.-2024, 23:59:00
Salaire (Base de paie) : 7 540,44Euro (EUR) Mensuelle
Grade NATO Grade G17

Description

"Sous Réserve d'approbation par les autorités budgétaires"

1. RÉSUMÉ

La directrice/Le directeur des systèmes d'information (CIO) de l'OTAN, par sa fonction, assure la cohérence des technologies de l'information et de la communication (TIC) au sein des organismes civils et militaires de l'entreprise OTAN. La/Le CIO de l'OTAN est chargé(e) de concrétiser la vision des Alliés pour l'entreprise OTAN. Elle/Il rend compte à la/au secrétaire général(e) et est responsable, à l'échelle de l'entreprise OTAN, de l'élaboration des directives et de la formulation des avis concernant l'acquisition et l'utilisation des technologies de l'information et des services informatiques. Elle/Il assure la supervision des questions de cybersécurité à l'échelle de l'entreprise OTAN et, en étroite coordination avec tous les organismes civils et militaires compétents de l'Organisation, s'emploie à améliorer constamment l'hygiène informatique et la posture de cybersécurité de l'entreprise.

Le Bureau de la/du CIO (OCIO) est une entité composite regroupant des membres du Secrétariat international (SI) et de l'État-major militaire international (EMI). L'OCIO contribue à la planification, à la coordination et à l'exécution des opérations cybernétiques défensives (DCO) sur les réseaux de l'OTAN, en sa qualité de membre de premier plan de la Cellule Planification et coordination des opérations cybernétiques défensives (DPCC). La DPCC comprend des représentants du Centre des cyberopérations (CyOC), de la Division civilo-militaire Renseignement et sécurité (JISD), de l'Agence OTAN d'information et de communication (NCIA) et de l'OCIO.

La Branche Sécurité des systèmes numériques d'entreprise (ESEC) supervise les questions de cybersécurité à l'échelle de l'entreprise OTAN et mène des actions de sensibilisation à certains risques, processus et incidents. Elle aide la/le CIO à gérer les risques et incidents de cybersécurité à l'échelle de l'entreprise OTAN, remet des avis et concourt au processus décisionnel lorsqu'il s'agit d'identifier la propension au risque et la tolérance au risque. Elle exécute des fonctions découlant des rôles de propriétaire du risque et de principal gestionnaire des incidents en matière de cybersécurité pour l'entreprise OTAN ; elle coordonne ainsi la réponse aux incidents, les analyses d'incidences métier, l'atténuation des risques, les mesures à moyen et long terme et les enseignements tirés. Elle entretient également des relations avec des parties prenantes civiles et militaires clés aux niveaux stratégique, opératif, tactique et technique.

La Section Processus de sécurité des systèmes numériques (SPS) a pour mission d'apporter à de multiples acteurs OTAN compétents dans le domaine du cyberespace un soutien et une représentation corrects, en sa qualité de gestionnaire des incidents pour l'entreprise OTAN. Elle a également pour tâche d'assurer la liaison avec les entités responsables de la sécurité des réseaux, de l'analyse des menaces et des opérations techniques avancées à l'appui de la défense des réseaux, services et capacités de l'entreprise OTAN.

La/Le titulaire du poste est chargé(e) de coordonner les travaux de la DPCC, en veillant à ce que les acteurs concernés de l'entreprise OTAN (CyOC, JISD et NCIA) communiquent et coopèrent de manière appropriée et en temps opportun. Elle/Il est chargé(e) de gérer le cycle de vie complet des DCO, y compris les phases de proposition, de planification, de conduite, d'évaluation et de suivi définies dans le processus relatif aux DCO. Elle/Il contribue aux réunions de la DPCC, facilite les débats et participe au processus de prise de décision. Elle/Il élabore et pilote les activités ayant trait aux DCO en assurant une coordination étroite avec les processus de gestion des incidents cyber et de gestion des risques cyber.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La/Le titulaire du poste doit :

- posséder un diplôme universitaire, ou une qualification équivalente, délivré par un institut de valeur reconnue, de préférence dans le domaine des TIC ou dans un domaine en lien avec la cybersécurité ;
- avoir au moins trois années d'expérience dans le domaine de la cybersécurité, acquise de préférence au sein d'une grande organisation ;
- avoir une expérience s'agissant de gérer le développement et la mise en œuvre de capacités de cybersécurité et des processus de sécurité associés ;
- avoir une expérience s'agissant d'élaborer et de mettre en œuvre des processus et des procédures à l'appui des opérations techniques avancées ;
- avoir une bonne connaissance et une solide expérience de la planification, de la coordination et de l'exécution des opérations techniques avancées, notamment des activités de chasse aux menaces et des technologies de tromperie et d'émulation d'attaque ;
- avoir une bonne connaissance des bonnes pratiques et des processus en matière de gestion des incidents cyber et de gestion des risques cyber ;
- avoir une bonne connaissance des principes de sécurité des réseaux et des infrastructures applicables à la cybersécurité ;
- avoir une bonne connaissance des principes, de la politique et des procédures applicables à la cybersécurité, acquise de préférence dans des organisations militaires et/ou de défense ;
- être capable de préparer et de présenter des exposés et des rapports clairs et concis à un public de spécialistes ou de non-spécialistes ;
- avoir de solides compétences en matière de gestion des parties prenantes ;
- posséder d'excellentes capacités d'analyse et de résolution de problèmes, ainsi que de communication, tant à l'oral qu'à l'écrit ;

- avoir au minimum le niveau de compétence V (« avancé ») dans l'une des deux langues officielles de l'OTAN (anglais/français), et le niveau I (« débutant ») dans l'autre ;
- savoir faire preuve de flexibilité et être disposé(e) à travailler en dehors des heures normales de service, durant les activités liées à la gestion d'un incident, et être apte et disposé(e) à effectuer des déplacements lorsqu'il y a lieu.

ACQUIS SOUHAITABLES

Seraient considérés comme autant d'atouts :

- des certifications en cybersécurité telles que CISSP, CCSP ou CISM, ou un diplôme de troisième cycle équivalent dans le domaine de la cybersécurité ;
- une expérience de l'environnement de cybersécurité de l'OTAN, en particulier dans des fonctions en lien avec la sécurité des SIC ou dans des fonctions connexes ;
- une expérience du travail sur des projets complexes et de la coordination d'acteurs multiples sur des sites distincts ;
- une expérience professionnelle dans une organisation internationale complexe ;
- une compréhension du fonctionnement de l'OTAN, de sa politique de sécurité et de ses directives complémentaires ;
- une bonne compréhension des TIC actuelles et émergentes et de la manière dont les entreprises les emploient pour développer l'activité numérique.

3. RESPONSABILITÉS PRINCIPALES

Voir la version anglaise.

4. STRUCTURE ET LIAISONS

La/Le titulaire du poste relève de la/du chef de la Section Processus de sécurité des systèmes numériques. Elle/Il travaille en étroite coopération avec les autres membres du personnel de l'OCIO ainsi qu'avec des experts des diverses entités OTAN.

Nombre de subordonné(e)s direct(e)s : sans objet.

Nombre de subordonné(e)s indirect(e)s : sans objet.

5. COMPÉTENCES

La/Le titulaire du poste doit faire preuve des compétences suivantes :

- Réflexion analytique : discerne les relations multiples.
- Flexibilité : s'adapte à des situations imprévues.
- Persuasion et influence : prend différentes mesures à des fins de persuasion.
- Initiative : fait preuve de décision dans les situations où il faut agir sans attendre.
- Compréhension organisationnelle : comprend le climat et la culture de l'Organisation.
- Travail en équipe : coopère.

6. CONTRAT

Contrat proposé (hors détachement) : contrat d'une durée déterminée de trois ans ; renouvelable pour une période de trois ans maximum, au cours de laquelle le/la titulaire pourra demander qu'il soit transformé en contrat de durée indéterminée.

Clause contractuelle applicable :
Conformément à la politique des contrats, il s'agit d'un poste auquel il est souhaitable, pour des raisons politiques, d'assurer une rotation de manière à pouvoir répondre au besoin qu'a l'Organisation d'exécuter les tâches qui lui sont confiées par les pays dans un environnement en constante évolution, notamment en préservant la souplesse nécessaire à l'adaptation de son profil de compétences, et de veiller au degré de diversité approprié à son caractère international.

La durée de service maximale prévue à ce poste est de six ans. La personne retenue se verra offrir un contrat d'une durée déterminée de trois ans, qui pourra être reconduit pour une période de trois ans maximum. Toutefois, conformément à la procédure décrite dans la politique des contrats, elle pourra demander, au plus tard un an avant l'expiration de la deuxième période, que son contrat soit transformé en contrat de durée indéterminée.

Si la personne retenue est détachée de l'administration d'un État membre de l'OTAN, elle se verra offrir un contrat d'une durée déterminée de trois ans, qui, sous réserve de l'accord des autorités nationales concernées, pourra être reconduit pour une période de trois ans maximum. À ce poste, la durée de service d'un agent détaché n'excède pas six ans.
Les agents en fonction se verront offrir un contrat conforme aux dispositions du Règlement du personnel civil de l'OTAN.

7. INFORMATIONS UTILES CONCERNANT LA PROCÉDURE DE CANDIDATURE ET DE RECRUTEMENT

On notera que seules les candidatures de ressortissant(e)s de pays de l'OTAN pourront être acceptées. Les candidatures doivent être soumises comme suit :

- pour les seuls agents civils de l'OTAN : via le portail de recrutement interne (lien) ;
- pour toutes les autres candidatures : via le lien www.nato.int/recruitment.

Il est recommandé de commencer par regarder ici une vidéo proposant six conseils destinés à aider les candidat(e)s à préparer leur dossier.

En outre, on trouvera ici une vidéo expliquant la marche à suivre sur le portail pour introduire son dossier de candidature et s'assurer de sa réception par l'OTAN dans les délais fixés.

On trouvera de plus amples informations concernant le processus de recrutement et les conditions d'emploi sur le site web de l'OTAN (http://www.nato.int/cps/fr/natolive/recruit-hq-e.htm).

La nomination se fera après vérification des diplômes et des antécédents professionnels de la/du candidat(e) retenu(e) et sous réserve de la délivrance d'une **habilitation de sécurité** par les autorités du pays dont la/le candidat(e) retenu(e) est ressortissant(e), de l'approbation de son **dossier médical** par la/le médecin-conseil de l'OTAN et de l'achèvement du processus d'**accréditation** et de notification par les autorités compétentes.

Dans le cadre de ses procédures de recrutement et de sélection, l'OTAN n'acceptera aucune réponse qui aura été produite, en tout ou en partie, au moyen d'un outil d'intelligence artificielle (IA) générative, notamment d'un modèle conversationnel comme ChatGPT (*Chat Generative Pre-trained Transformer*) ou de tout autre générateur de texte. L'Organisation se réserve le droit de vérifier si la/le candidat(e) a eu recours à de tels outils. Tout dossier de candidature élaboré, en tout ou en partie, à l'aide d'une application d'IA générative ou créative pourra être rejeté sans autre examen, à la seule discrétion de l'OTAN. Cette dernière se réserve également le droit de prendre toute autre mesure qu'elle jugerait nécessaire.

8. INFORMATIONS COMPLÉMENTAIRES

L'OTAN est déterminée à promouvoir la diversité et l'inclusion, et elle s'attache à assurer l'égalité de traitement en matière d'emploi, d'avancement et de fidélisation indépendamment de toute considération liée au genre, à l'âge, à la nationalité, à l'origine ethnique, à la religion ou aux croyances, à la culture, à l'orientation sexuelle, ou au handicap. L'Organisation examinera les candidatures de ressortissant(e)s de tous les pays membres, et encourage vivement les femmes à postuler.

Le développement de l'intégrité est un élément clé des tâches fondamentales de l'Alliance. En tant qu'employeur, l'OTAN attache une grande importance au respect des principes d'intégrité, de transparence et de redevabilité, conformément aux normes et aux pratiques internationales établies pour le secteur de la défense et de la sécurité s'y rapportant. Les candidat(e)s sélectionné(e)s doivent être des modèles d'intégrité et s'employer en permanence à promouvoir la bonne gouvernance dans le cadre de leur travail.

En raison du vif intérêt suscité par l'OTAN et du nombre élevé de candidatures potentielles, il ne pourra pas être donné suite aux demandes de renseignements adressées par téléphone ou par courrier électronique.

Les candidat(e)s qui ne seront pas retenu(e)s pour ce poste pourront se voir offrir un poste analogue, au même grade ou à un grade inférieur, pour autant qu'ils/elles remplissent les conditions requises.

De par la nature du poste, le/la titulaire peut parfois être amené(e) à voyager pour le travail et/ou à travailler en dehors des heures normales de service.

L'Organisation, en application de plusieurs politiques sur l'équilibre entre vie professionnelle et vie privée, propose notamment des possibilités de télétravail et d'horaire flexible sous réserve des exigences liées à la fonction.

Le Secrétariat international de l'OTAN est un environnement sans tabac.

Pour en savoir plus sur l’échelle unique de rémunération mise en place à l’OTAN (grades, indemnités, etc.), veuillez consulter notre site web. Des informations détaillées sont fournies sous l'onglet Salaires et allocations.