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, Cyber Resilience (241845)

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 26-Jan-2025
Salary (Pay Basis): 7,504.44Euro (EUR) Monthly
Grade NATO Grade G17
Clearance Level NS

Description

'PENDING BUDGET APPROVAL'

1.SUMMARY

The NATO Chief Information Officer (CIO) function brings Information and Communications Technology (ICT) coherence across the 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 considering the implications of independent initiatives on the Enterprise.
The NATO CIO Office is an integrated staff organization comprising members of the International Staff (IS) and the International Military Staff (IMS).

The Enterprise Security Branch (ESB) maintains Enterprise oversight on cyber security and enables cyber awareness by interfacing with the main NATO cybersecurity entities. It supports the CIO in managing cybersecurity risks and incidents at Enterprise level, advises and supports the decision-making process for setting the Enterprise risk appetite and risk acceptance for CIS Security. In particular, the Branch supports the CIO's role of Enterprise risk owner and Enterprise incident manager for cybersecurity, coordinating immediate response, business impact analysis, risk mitigation, mid- to long-term mitigation measures and lessons-identified definition.

The Enterprise Risk Management Section (ESRM) is responsible for ensuring the execution of the Enterprise CIS Operational Authority (CISOA) role across NATO, adopting a modern and effective risk management methodology, driving activities of other Enterprise cybersecurity processes (Incident Management and Defensive Cyberspace Operations (DCO)). The Section also offers support to accreditation efforts for NATO CISs at Enterprise Level, including the coordination of

auditing activities, provision of Cryptographic support, Personal Data Protection policy changes for the Enterprise.
The incumbent is responsible for building resilience and supporting the three Enterprise cybersecurity processes (Risk Management, Incident Management and Defensive Cyber Operations), as well as supporting to enhance\innovate the capacity of these processes whenever dictated by resources constraints. The incumbent also takes the role, when required, of Risk Manager in support of risk-driven activities (such as Incident Management and DCOs), and the development of analyses and assessments which are instrumental for risk-based decision-making of the CIO as Single Point of Authority (SPA) of NATO Cybersecurity.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- possess a degree from a university or from an institute of recognised standing preferably in ICT or related discipline;
- have at least 3 years of experience in the Cybersecurity field, preferably in large international organizations;
- have demonstrated experience in Risk Management-related activities, preferably in support of different cybersecurity processes such as Incident Management, Risk Management or Cyber Operations;
- have strong written and oral communication skills, including the ability to draft documents and presentations for a senior audience;
- possess knowledge and experience in coordinating with multiple stakeholders in large, decentralized and multi-cultural organizations;
- possess a good knowledge of the principles, policy and procedures governing cyber defence;
- have the ability to draft clear and concise reports, produce and maintain security and risks' logs and databases in support of security activities;
- demonstrate sound political judgement;
- have experience in writing speeches and speaking notes for senior officials;
- have competencies with off-the-shelf MS software (e.g. MS Excel, Word, Outlook, SharePoint and PowerPoint);
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; I ("Beginner") in the other;
- be flexible to work outside of normal office hours and travel when required.

DESIRABLE

The following would be considered an advantage:

- knowledge and experience in supporting the activities of Defensive Cyberspace Operations;
- knowledge of the NATO organization and its cybersecurity policy and supporting directives.

3. MAIN ACCOUNTABILITIES

Planning and Execution

Prepare, plan and organise the Board of CIS Operational Authorities (BCISOA), Cyber Risk Management Group (CRMG)'s meetings. Draft, coordinate and distribute agendas, share the documents and presentations with the stakeholders across the NATO Enterprise, and draft the minutes of the meetings. Augment the Risk Management activities in support of Risk-based decision making of the Enterprise CISOA, the execution of Incident Management and Defensive Cyber Operations. Support the development of High-Level risk assessments instrumental for risk-based decisions within the three cybersecurity processes (RM, IM and DCOs), collecting and analyzing all available technical information and resources, acting as "Risk Management SME" in the execution of various risk management activities. Provide risk-based assessments and recommendations to facilitate HOTO between IM and DCOs processes with Risk Management and act as Risk Management SME in the execution of the abovementioned cybersecurity processes as resilience-building mechanism.

Knowledge Management

Organize, administrate and directly contribute to the sharing and distributing of information and knowledge within the office and with stakeholders across the NATO Enterprise, using tools such as MS SharePoint, MS Outlook, and the tasker tracker systems. Draft memoranda and cover letters to documents. On the basis of briefings, discussions and investigations, assess the security programs in place in NATO nations, NATO civil and military bodies, and non-NATO nations / international organizations. Develop and maintain a log of the non-accredited systems and assess the status of the accreditation process at Enterprise level, possibly making suggestions and plans to improve it. In cooperation with OCIO staff and points of contacts across the NATO Enterprise, develop and enhance knowledge related to sharing and distributing information. Maintain an effective follow-up and/or reminder system for pending actions. Control the quality, quantity and relevance of input to the knowledge management systems. Draft speeches and speaking notes for senior officials. Type and format all kinds of documents, using the standard software packages used by NATO (MS Word, Excel, and PowerPoint).

Stakeholder Management

Interact with high-level Boards to facilitate risk-informed decisions. Write comprehensive reports for the use of responsible national and/or security authorities. Coordinate activities in support of the work of decision-making Boards. Liaise and cooperate with the NATO Enterprise entities points of contact (International Staff, International Military Staff, Agencies and other NATO bodies) with regard to meetings' planning, preparation and running. Develop contacts and cooperation in support of the conduct of the BCISOA and CRMG activities. Maintain accurate lists of stakeholders for information exchange. Clarify and contribute to stakeholders' expectations. Represent the CIO across different Boards, Groups and Committees, including the NATO CIS Security Accreditation Board (NSAB), the Senior Executive Group (SEG), the Cyber Defense Committee (CDC), as well as working groups, including the BCISOA Working Group and the Cyber Risk Management Group as directed by the Head

Expertise Development

Contribute to enhancing processes and procedures that improve the overall functioning of the NATO Enterprise. Maintain and apply expertise regarding the initiatives tracked via the BCISOA and CRMG and other committees they support. Provide Cybersecurity advice and guidance to the

section head, on the basis of the performance of the three cybersecurity processes, perceived threats, current resources status and vulnerabilities for the Enterprise. Prepare advice to the OCIO management regarding their participation and contribution to the respective meetings.

Project Management

Oversee and monitor the execution of assigned projects in support of the OCIO goals and objectives and provide specialist input where required.
Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

The incumbent reports to the Section Head, Enterprise Risk Management. The incumbent deals with senior government and military personnel in NATO and partner nations, NATO civil and military bodies, and non-NATO nations and organizations.
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 (cyberrésilience) (241845)

Emplacement principal : Belgique-Bruxelles
Organisation :OTAN SI
Horaire : Temps plein
Date de retrait :26-janv.-2025
Salaire (Base de paie) :7 504,44Euro (EUR) Mensuelle
Grade NATO Grade G17
Niveau de l'habilitation de sécurité NS

Description

“SOUS RÉSERVE D'APPROBATION PAR LES AUTORITÉS BUDGÉTAIRES”

1.RÉSUMÉ

La fonction de directrice/directeur des systèmes d’information (CIO) de l’OTAN 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 de l'élaboration des directives et de la formulation des avis à l’échelle de l’entreprise en ce qui concerne l’acquisition et l’utilisation des technologies de l’information et des services informatiques, en prenant en compte les incidences que des initiatives indépendantes pourraient avoir pour l'OTAN dans son ensemble.
Le Bureau de la/du CIO est une entité composite regroupant des membres du Secrétariat international (SI) et de l’État-major militaire international (EMI).
La Branche Sécurité des systèmes numériques d’entreprise (ESB) assure la supervision de la cybersécurité à l’échelle de l’entreprise, et favorise la sensibilisation à la cybersécurité en interagissant avec les principales entités OTAN concernées. Elle aide la/le CIO à gérer les risques et incidents de cybersécurité à l’échelle de l’entreprise OTAN, formule des avis et concourt au processus décisionnel lorsqu'il s’agit de déterminer le rapport au risque et le niveau de risque acceptable dans l’entreprise pour ce qui est de la sécurité des SIC. Elle soutient en particulier la/le CIO dans ses 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’impact sur l’activité, l’atténuation des risques, les mesures d’atténuation à moyen et long terme et la définition des enseignements tirés.
La Section Gestion des risques assure l’exécution du rôle d’autorité opérationnelle des SIC (CISOA) pour l’ensemble de l’entreprise OTAN ; elle adopte pour ce faire une méthode moderne et efficace de gestion des risques, laquelle sous-tend les activités découlant des autres processus de l’entreprise OTAN relatifs à la cybersécurité (gestion

des incidents et DCO). Elle contribue aussi aux activités d'homologation des SIC de l'OTAN à l'échelle de l'entreprise, y compris à la coordination des activités d'audit, à la fourniture d'un soutien en matière de cryptographie et à l'exécution de modifications à la politique sur la protection des données à caractère personnel pour l'entreprise.
La/Le titulaire du poste est chargé(e) de renforcer la résilience et de soutenir les trois processus de cybersécurité de l'entreprise (gestion des risques, gestion des incidents et cyberopérations défensives), ainsi que de contribuer au renforcement de ces processus et d'intégrer des innovations dans les capacités correspondantes chaque fois que cela est dicté par des contraintes de ressources. La/le titulaire(e) assume également le rôle de gestionnaire des risques, selon les besoins, à l'appui des activités axées sur les risques (telles que la gestion des incidents et les DCO) et de l'élaboration d'analyses et d'évaluations qui sont essentielles pour la prise de décisions fondées sur les risques par le CIO, autorité unique pour la cybersécurité à l'OTAN.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La/Le titulaire du poste doit:

- être diplômé(e) d'une université ou d'un établissement de valeur reconnue, de préférence dans le domaine des TIC, ou dans une autre discipline pertinente ;
- avoir au moins trois années d'expérience dans le domaine de la cybersécurité, acquise de préférence au sein d'une organisation internationale ;
- avoir une expérience avérée des activités liées à la gestion des risques, de préférence à l'appui de différents processus de cybersécurité tels que la gestion des incidents, la gestion des risques ou les cyberopérations ;
- avoir d'excellentes aptitudes à la communication écrite et orale, y compris la capacité de rédiger des documents et d'élaborer des exposés à l'intention de hauts responsables ;
- avoir une connaissance et une expérience de la coordination de groupes d'intervenants multiples, acquises dans des organisations multiculturelles décentralisées et de grande envergure ;
- avoir une bonne connaissance des principes, des politiques et des procédures qui régissent les activités de cyberdéfense ;
- être capable de rédiger des rapports clairs et concis ainsi que de produire et de tenir à jour des journaux et des bases de données concernant la sécurité et les risques, à l'appui d'activités relatives à la sécurité:
- faire preuve d'un jugement politique sûr:
- avoir une expérience de la rédaction de discours et de notes d'orateur pour de hauts responsables:
- savoir utiliser les logiciels d'une suite bureautique (p. ex. MS Excel, MS Word, MS Outlook et MS PowerPoint):
- 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
- être disposé(e) à travailler en dehors des heures normales de service et à effectuer des déplacements lorsqu'il y a lieu.

ACQUIS SOUHAITABLES

- Seraient considérées comme autant d'atouts :
- une connaissance et une expérience du soutien aux activités menées au titre des opérations défensives dans le cyberespace ;
- une connaissance de l'OTAN, de sa politique de cybersécurité et de ses directives complémentaires.

3. RESPONSABILITÉS PRINCIPALES

Planification et exécution

Prépare, planifie et organise les réunions du Comité des autorités opérationnelles SIC (BCISOA)/Groupe de gestion des risques cybernétiques (CRMG). Elle/il établit, coordonne et diffuse les ordres du jour, partage les documents et les présentations avec les parties prenantes dans l'ensemble de l'entreprise OTAN et rédige les comptes rendus de réunion. Renforce les activités de gestion des risques à l'appui de la prise de décision fondée sur les risques de la CISOA de l'entreprise, de la gestion des incidents et des opérations cybernétiques défensives. Contribue à l'élaboration d'évaluations de haut niveau des risques – qui sont essentielles pour la prise de décisions fondées sur les risques dans le cadre des trois processus de cybersécurité (gestion des risques, gestion des incidents, DCO) – en recueillant et en analysant toutes les informations et ressources techniques disponibles, et en agissant en tant qu'expert(e) de la gestion des risques dans l'exécution de diverses activités de gestion des risques. Fournit des évaluations fondées sur les risques et des recommandations afin de faciliter la coordination entre les processus de la gestion de l'information et des DCO et la gestion des risques, et agit en tant qu'expert de la gestion des risques dans l'exécution des processus de cybersécurité susmentionnés, en tant que mécanisme de renforcement de la résilience.

Gestion des connaissances

Organise et gère tout ce qui touche à l'information et aux connaissances et contribue directement à leur partage et à leur diffusion au sein du Bureau et avec les différents acteurs de l'entreprise OTAN, en exploitant les outils à sa disposition comme MS SharePoint, MS Outlook et les systèmes de suivi des tâches. Rédige des mémorandums, ainsi que des lettres destinées à accompagner divers documents envoyés. À partir d'exposés, de débats et de recherches, procède à l'évaluation des programmes de sécurité en place dans les pays membres et les organismes civils et militaires de l'OTAN ainsi que dans des pays non OTAN et des organisations internationales. Établit et tient à jour un registre des systèmes non homologués et évalue l'état d'avancement du processus d'homologation au niveau de l'entreprise, en formulant éventuellement des suggestions et des plans pour l'améliorer. En coopération avec les membres de l'OCIO et les points de contact de toute l'entreprise OTAN, développe et améliore les connaissances en matière de partage et de diffusion de l'information. Applique un système efficace de suivi et/ou de rappel pour les tâches à exécuter. Contrôle la qualité, la quantité et la pertinence des données à introduire dans les systèmes de gestion des connaissances. Prépare des discours et des notes d'orateur pour de hauts responsables. Crée tout type de documents à l'aide des applications standard utilisées par l'OTAN (à savoir MS Word, MS Excel et MS PowerPoint) et met en page ces derniers.

Gestion des parties prenantes

Interagit avec les comités de haut niveau pour faciliter une prise de décision éclairée sur les risques. Établit des rapports complets destinés aux autorités nationales et/ou de sécurité compétentes. Coordonne les activités à l'appui des travaux des comités décisionnels. Se tient en liaison et coopère avec les points de contact des entités de l'entreprise OTAN (Secrétariat international, État-major militaire international, agences et autres organismes OTAN) pour ce qui concerne la planification, la préparation et la tenue des réunions. Établit des contacts et met en place une coopération qui facilitent la conduite des activités du BCISOA et du CRMG. Tient des listes précises des parties prenantes pour les besoins de l'échange d'informations. Cerne précisément les attentes des parties prenantes et contribue à y répondre. Représente la/le CIO au sein de différents conseils, groupes et comités, notamment le Bureau d'homologation de sécurité des SIC de l'OTAN (NSAB), le Groupe exécutif de haut niveau (SEG) et le Comité de cyberdéfense (CDC), ainsi que des groupes de travail, notamment le Groupe de travail du BCISOA et le CRMG, selon les instructions de la/du chef.

Développement de l'expertise

Contribue à l'optimisation des processus et des procédures qui permettent d'améliorer le fonctionnement général de l'entreprise OTAN. Entretient et exerce l'expertise qui est la sienne dans les initiatives qui font l'objet d'un suivi par le BCISOA et le CRMG ainsi que par les autres comités auxquels elle/il fournit un soutien. Fournit des avis et des orientations en matière de cybersécurité à la/au chef de Section, sur la base de la performance des trois processus de cybersécurité, des menaces perçues, de l'état actuel des ressources et des vulnérabilités de l'entreprise. Établit des avis à l'intention des gestionnaires de l'OCIO concernant leur participation et leur contribution aux différentes réunions.

Gestion de projet

Assure la supervision et le suivi des projets qui lui sont confiés et qui servent les buts et objectifs de l'OCIO. Apporte son expertise, s'il y a lieu.

S'acquitte de toute autre tâche en rapport avec ses fonctions qui pourrait lui être confiée.

4. STRUCTURE ET LIAISONS

La/Le titulaire du poste relève de la/du chef de la Section Gestion des risques de l'entreprise. Elle/Il est en contact avec de hauts responsables, gouvernementaux ou militaires, des pays de l'OTAN et des pays partenaires, d'organismes civils et militaires de l'OTAN et d'entités et organisations non 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