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

Senior Officer, Incident Management-240643

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 05-May-2024, 11:59:00 PM
Salary (Pay Basis): 8,754.21Euro (EUR) Monthly
Grade: NATO Grade G20

Description:

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 realise 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 cyber hygiene and cybersecurity posture of 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 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 NATO Enterprise cyber incident management and response activities involving NATO enterprise CIS and services. The incumbent ensures that the required activities are appropriately and timely coordinated across the Enterprise stakeholders, in accordance with NATO's Cyber Incident Response Plan (CIRP). The incumbent works in close coordination with the NATO Communications and Information Agency (NCIA), the Joint Intelligence and Security Division (JISD) the Cyberspace Operations Centre (CyOC), the NATO Cyber Risk Management Group (CRMG) and the NATO Board of CIS Operational Authorities (BCISOA). The incumbent is responsible for the update and maintenance of the Enterprise Incident Management framework and supporting processes.

The incumbent deputises for the Head, Security Processes Section, when required.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- hold 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 6 years of experience in cybersecurity;
- have extensive knowledge and experience in coordinating multiple stakeholders responses to cyber incidents in large, decentralized and multi-cultural organizations;
- have a good knowledge and experience in the cybersecurity domain and specifically in cyber incident response processes;
- have proven experience in the generation, provision and long-term assessment of cybersecurity recommendations and guidance originating from cyber incidents happening in and through cyberspace;
- have good knowledge of:
    - network and infrastructure security principles, along with best practices for implementing protective measures, monitoring and logging;
    - cyber risk management and advanced technical operations best practices and processes;
    - 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;

- have strong interpersonal skills, with a focus on stakeholders management;
- possess excellent analytical, problem solving, and verbal and written communication skills;
- be able to work under high pressure while preserving a teamwork spirit;
- posses 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 cyber incident management activities, and 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;
- experience building and leading a diverse team.

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 NATO Enterprise cyber incident management activities, processes and procedures. Provide advice and guidance to NATO Nations, NATO civil and military bodies, partner nations and international organisations. Develop high-level strategic documents and advice to support and improve the Enterprise cyber incident management processes and procedures.

Expertise Development

Maintain and update an Enterprise-wide cyber incident management framework to support the role of CIO as single point of authority for the Enterprise CIS. Based on the latest Security assessments and developments in cybersecurity threats, propose changes and improvements to the Framework, gathering ideas and lessons learned from other NATO experts across the Enterprise. Identify, develop and test new capabilities in support of Enterprise cyber incident management. 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.

Coordinate and develop the processes and procedures required to better support the different phases of the CIRP. Coordinate cyber incident response activities involving Enterprise CIS and assess their effectiveness under time pressure. Coordinate and propose mitigation and remediation actions in close collaboration with the relevant Enterprise stakeholders, bodies and groups.

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 Enterprise cyber incident management. 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 relevant NATO bodies and stakeholders (e.g. NATO Cyber Risk management Group (CRMG), the NATO Board of CISOA (BCISOA)) that contribute and support cyber incident management 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.

Financial Management

Manage a predetermined budget for assigned projects.

Representation of the Organization

Represent the Section at NATO and in various international settings, including in dialogues with government, civilian and military national representatives and giving presentations at conferences and seminars.

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. The incumbent leads a diverse team in charge of establishing strong relationships with the relevant NATO stakeholders that support cyber incident management activities across the NATO Enterprise.

Direct reports: N/A
Indirect reports: N/A

5. COMPETENCIES

The incumbent must demonstrate:

- Achievement: Creates own measures of excellence and improves performance.
- Analytical Thinking: Sees multiple relationships.
- Change Leadership: Expresses vision for change.
- Impact and Influence: Uses indirect influence.
- Initiative: Is decisive in a time-sensitive situation.
- Organisational Awareness: Understands organisational politics.
- Teamwork: Solicits inputs and encourages others.

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 sénior (gestion des incidents)-240643

Emplacement principal: Belgique-Bruxelles
Organisation: OTAN SI
Horaire: Temps plein
Date de retrait: 05-mai-2024, 23:59:00
Salaire (Base de paie): 8 754,21Euro (EUR) Mensuelle
Grade: NATO Grade G20

Description:

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, 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 concertation 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).

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 spécifiques. 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 intervenants 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 la coordination des activités de gestion et de réponse liées aux incidents cyber affectant les SIC et les services de l'entreprise OTAN. Elle/Il veille à ce que les activités requises soient coordonnées rapidement et comme il se doit entre les parties prenantes de l'entreprise OTAN, conformément au plan OTAN de réponse aux cyberincidents (CIRP). Elle/Il travaille en concertation étroite avec l'Agence OTAN d'information et de communication (NCIA), la Division civilo-militaire Renseignement et sécurité (JIS), le Centre des cyberopérations (CyOC), le Groupe de gestion du risque cyber (CRMG) et le Comité des autorités opérationnelles des SIC (BCISOA). Elle/Il est responsable de l'actualisation et de la maintenance du cadre de gestion des incidents de l'entreprise OTAN et des processus associés à celui-ci.

La/Le titulaire du poste supplée la/le chef de la Section Processus de sécurité des systèmes numériques en cas de besoin.

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 6 ans d'expérience dans le domaine de la cybersécurité ;
- avoir une connaissance théorique et pratique approfondie de la coordination des réponses d'intervenants multiples aux incidents cyber, et l'avoir acquise de préférence dans des organisations multiculturelles décentralisées et de grande envergure ;
- avoir une bonne connaissance théorique et pratique du domaine de la cybersécurité, et plus spécifiquement des processus de réponse aux incidents cyber ;
- avoir déjà formulé, fourni et évalué sur la durée des recommandations et des orientations en matière de cybersécurité découlant d'incidents survenus dans et à travers le cyberespace ;
- avoir une bonne connaissance :
  - des principes sous-tendant la sécurité des réseaux et des infrastructures, ainsi que des bonnes pratiques en matière d'application de mesures de protection, de surveillance et de journalisation ;

    - des bonnes pratiques et des processus en matière de gestion des risques cyber et d'opérations techniques avancées ;
    - des principes, de la politique et des procédures applicables à la cybersécurité, connaissance qu'elle/il aura 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 très bonnes compétences relationnelles, en particulier dans le domaine de la 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 ;
- être capable de travailler sous haute pression tout en veillant à préserver l'esprit d'équipe;
- 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 cyber, ainsi qu'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 des directives complémentaires à celle-ci ;
- une expérience de la mise en place et de la direction d'une équipe composée de profils variés.

3. RESPONSABILITÉS PRINCIPALES

Élaboration des politiques

Contribue à l'élaboration des politiques, des directives et des documents d'orientation dans les domaines de responsabilité de l'OCIO qui relèvent de ses compétences. Donne à la/au chef de la Section des avis sur les activités, processus et procédures de gestion des incidents cyber à l'échelle de l'entreprise OTAN. Remet des avis et des orientations aux pays membres et aux organismes civils et militaires de l'OTAN, ainsi qu'aux pays partenaires et à des organisations internationales. Établit des documents stratégiques de haut niveau et des avis visant à soutenir et améliorer les processus et procédures de l'entreprise OTAN ayant trait à la gestion des incidents cyber.

Développement de l'expertise

Tient à jour et actualise un cadre pour la gestion des incidents cyber à l'échelle de l'entreprise à l'appui du rôle de la/du CIO en tant qu'autorité unique pour les SIC de l'entreprise OTAN. Formule des propositions de modification et d'amélioration de ce cadre, sur la base des dernières évaluations de sécurité et des développements les plus récents relatifs aux menaces en matière de cybersécurité, en rassemblant à cet effet les idées et les enseignements provenant d'autres experts de l'entreprise OTAN. Recherche, développe et met à l'essai de nouvelles capacités à l'appui de la gestion des incidents par l'entreprise OTAN. Se tient informé(e) des développements technologiques les plus récents dans son domaine de compétence, et formule des avis appropriés. Propose des mises à jour et des améliorations sur la base des enseignements identifiés lors de situations réelles et d'exercices.

Coordonne et développe les processus et les procédures nécessaires à une meilleure mise en œuvre des différentes phases du CIRP. Coordonne les activités de réponse aux incidents cyber affectant les SIC de l'entreprise OTAN et évalue leur efficacité dans les situations où le facteur temps est important. Propose des mesures d'atténuation et de correction, et en assure la coordination en étroite collaboration avec les acteurs, organismes et groupes concernés de l'entreprise OTAN.

Gestion de projet

Contribue à la définition du plan de projets de la Section, dans le respect du/des rôles dévolus à l'OCIO dans les processus de gestion de projet utilisés au sein de l'entreprise OTAN. Identifie les principaux décideurs et autres acteurs nécessaires à la réussite des projets. Participe et contribue aux travaux des comités de gestion des projets lorsqu'il y a lieu. Se tient parfaitement au fait des plans de projets et de programmes, identifie les risques pesant sur la mise en œuvre des projets et en assure le suivi, et met son expertise et son leadership au service de la gestion des exceptions et de la résolution des problèmes. Établit et entretient un réseau de relations avec les principaux chefs de projet au sein de l'entreprise OTAN, en particulier pour les projets ayant trait aux TIC et à la cybersécurité.

Gestion des parties prenantes

Établit et entretient un réseau de relations avec les principaux experts au sein de l'entreprise OTAN, en particulier pour la sécurité à l'échelle de l'entreprise. Entretient une coopération et des relations de travail étroites avec les acteurs OTAN impliqués dans le cycle de vie des processus et pratiques de sécurité de l'entreprise OTAN, et plus particulièrement dans la gestion des incidents cyber. Se sent à l'aise lorsqu'il s'agit de présider des organes et des comités exécutifs ou de haut niveau, de leur apporter un soutien et d'interagir avec eux.

Gestion des connaissances

Rédige des notes d'information et des rapports d'activité et prépare des présentations et d'autres documents pour des réunions de haut niveau. Contribue au partage de l'information avec les organismes et acteurs de l'OTAN qui contribuent aux activités de gestion des incidents cyber (p. ex. Groupe de gestion du risque cyber (CRMG), Comité des autorités opérationnelles des SIC (BCISOA)). À partir d'exposés, de débats et de recherches, formule des avis sur l'évolution des programmes de sécurité dans les pays membres et les organismes civils et militaires de l'OTAN ainsi que dans des entités non OTAN.

Gestion financière

Gère un budget prédéfini pour les activités qui lui sont confiées.

Représentation de l'Organisation

Représente la Section au sein de l'OTAN et dans diverses instances internationales, notamment en prenant part aux dialogues avec les gouvernements et les représentants civils et militaires des pays, et en faisant des exposés à des conférences et des séminaires.

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. Elle/Il dirige une équipe composée de profils variés qui est chargée d'établir de solides relations avec les acteurs de l'OTAN qui soutiennent les activités de gestion des incidents cyber à l'échelle de l'entreprise 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 :

- Recherche de l'excellence : crée ses propres critères d'excellence et améliore les performances.
- Réflexion analytique : discerne les relations multiples.
- Promotion du changement : exprime une vision pour le changement.
- Persuasion et influence : a recours à des techniques d'influence indirectes.
- Initiative : fait preuve de décision dans les situations où il faut agir sans attendre.
- Compréhension organisationnelle : comprend les rouages de l'Organisation.
- Travail en équipe : sollicite des contributions et encourage les autres.

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

Voir la version anglaise

8. INFORMATIONS COMPLÉMENTAIRES

Voir la version anglaise