

JOB DESCRIPTION

Deputy Chief Information Officer

NATO Communications and Information Agency (NCIA)

To strengthen the Alliance through connecting its forces, the NCIA delivers secure, coherent, cost-effective and interoperable communications and information systems in support of consultation, command and control, and enabling intelligence, surveillance and reconnaissance capabilities for NATO, where and when required. It includes IT support to the Alliance's business processes, including the provision of shared IT services to NATO Headquarters, the Command Structure and NATO Agencies.

The Chief Information Office (CIO) provides the strategic leadership, governance and enterprise capabilities required to deliver secure, resilient and modern information and communication technologies across the Agency. It is responsible for the Agency's technology strategy, digital enterprise, cyber security governance and the alignment of technology capabilities with NATO policy and the NCIA Strategic Plan.

The Deputy Chief Information Officer (Deputy CIO) owns NATO's operational cyber security, as a collateral duty they additionally support the Chief Information Officer in the leadership, management and continuous evolution of the Agency's information management systems, infrastructure, platforms, and digital capabilities. The Deputy CIO provides senior leadership across the CIO organisation, ensuring the effective implementation of the CIO's technology strategy, operating model and priorities through organisational leadership, people development, enterprise risk management, oversight of major initiatives and strategic supplier relationships.

The Deputy CIO serves as the CIO's principal advisor on cyber security and provides executive leadership for the Agency's cyber security capabilities. The role is responsible for leading and coordinating the Agency's cyber security functions, including those historically delivered through the NATO Cyber Security Centre (NCSC), ensuring the coherent implementation of cyber security policy and the integration of cyber security, cyber defence, cyber operations, vulnerability management, identity and access management, configuration security, and cyber risk management across the Agency.

As a member of the CIO senior leadership team, the incumbent contributes to Agency planning, supports the delivery of the NCIA Strategic Plan, represents the CIO in engagements with senior Agency and NATO stakeholders as required, and acts on behalf of the CIO in the exercise of delegated authority.

Duties:

Under the direction of Chief Information Officer, the incumbent will perform duties such as the following:

Leadership

- Embodiment and role model the NCIA culture principles of Customer First, Together and Impact
- Lead with the customer at the centre of every decision, build bridges across organizational pillars and drive delivery with the ownership and pace the mission demands
- Provide strategic and actionable direction in support of NCIA strategic and operational initiatives
- Represent the NCIA, as required, in Agency Governance Bodies, committees, meetings and conferences to promote NCIA interests, strategic goals
- Build, maintain and strengthen relations with internal and external stakeholders, modelling collaborative, customer-first behaviours, to optimally mobilise resources and commitments in support of relevant NCIA strategic priorities
- Build and lead a cohesive, multicultural and multidisciplinary team, promoting excellence, the highest professional standards and create psychologically safe work environments that enable managers and staff to develop their full potential
- Establish and maintain high-level working relationships with leadership across the NCIA and the NATO Enterprise to efficiently deliver and cooperate on corporate initiatives through trust and alignment
- Lead, motivate and contribute to the professional development and performance management of Agency staff, holding oneself and others accountable for delivery and high-quality work within set deadlines, efficient working methods and a constructive working atmosphere
- Ensure optimal utilization of available resources, prioritizing speed, agility and decisiveness, to meet the commitments of the Agency in the conduct of its work

Leadership of CIO Operations and Capabilities

- Deputise for the CIO and other senior leadership as required
- Act on behalf of the CIO, as delegated, representing the CIO in Agency governance bodies, senior stakeholder engagements and other internal and external forums
- Act as the technical lead for enterprise digital backbone strategy and architecture (including internal IT), ensuring technology initiatives, roadmaps, and capability design align with CIO-defined enterprise objectives
- Provide leadership for enterprise platforms, including cloud, on-premises, and hybrid environments, ensuring scalability, resilience, interoperability, and cost efficiency across the digital backbone
- Assume oversight of enterprise applications and business systems across the digital backbone, guiding selection, integration, modernisation, optimisation, and lifecycle management
- Drive digital enablement and process optimisation through automation, modern tooling, and emerging technologies across both enterprise backbone services and internal IT functions
- Provide expert technical advice to executive leadership on emerging technologies, risks, and opportunities, translating enterprise digital backbone strategy into implementable technical options
- Provide SME input into vendor and technology portfolio management across the enterprise digital backbone, ensuring alignment with CIO strategy and architectural standards

- Act as delegated technical authority for coherence and integration across infrastructure, applications, security, and service lifecycle domains within the digital backbone
- Perform other duties as may be required

Cyber Security Leadership

- Provide executive leadership for the Agency's cyber security capabilities, ensuring the coherent implementation of cyber security policy as defined by the NATO Digital Policy Committee, governance and risk management, including the functions historically delivered through the NATO Cyber Security Centre (NCSC)
- Promote the integration of cyber security, cyber defence and cyber resilience across the Agency's technology, platforms and digital services
- Act as SME for Cyber and Information Security (CIS), including enterprise security architecture, identity and access management, and security-by-design principles, ensuring alignment with CIO-defined risk posture and security policy
- Support the CIO in providing strategic leadership for the Agency's enterprise technology and cyber security capabilities, ensuring alignment with the NCIA Strategic Plan, NATO policy and Agency priorities

Experience and Education:

- A Master's degree at a nationally recognised/certified university in computer science, engineering, information systems, business management, or related field and 10 years post-related experience. Alternatively, a Bachelor's degree with 15 years post related experience;
- Proven experience in a senior IT leadership role within a large, complex technology organization
- Demonstrable experience leading the development and implementation of enterprise-wide technology strategies aligned with organizational objectives
- Experience overseeing the delivery and operation of large-scale IT services, including infrastructure, cloud services, enterprise applications, and cybersecurity, which support 1000+ users across multiple locations
- Proven track record of delivering major technology transformation programs, including cloud migration, modernization of legacy systems, digital workplace initiatives, or operating model transformation.
- Strong understanding of modern digital architectures, including:
 - Proven experience running contemporary CIS cloud-based workloads
 - IT/Digital strategy development and its implementation
 - All Lifecycle aspects of Information Systems
- Experience leading hybrid or multi-cloud environments and modern digital platforms.
- Familiarity with data governance, analytics, artificial intelligence, and emerging technology adoption
- Extensive cybersecurity expertise (10+ years) including strategic design of cyber-defence capabilities
- Modern security methodologies such as MITRE ATT&CK and Zero Trust
- Experience with cybersecurity and integration of security with engineering, architecture, and product disciplines.
- Experience leading cybersecurity, resilience, and information protection initiatives, ensuring compliance with regulatory and organizational requirements

- Strong experience in IT governance, portfolio management, risk management, and technology investment planning
- Proven experience establishing and improving IT service delivery and operational excellence, including the use of modern service management frameworks and performance metrics
- Experience managing significant operating and capital budgets (100M+ EUR) and optimizing technology investments to deliver measurable business value
- Proven experience in managing large, diverse and multidisciplinary teams, successfully employing modern, inspirational leadership practices
- Demonstrated success embedding a performance-driven culture through aligned goal setting and shared accountability across teams and direct reports

Desirable Experience and Education:

- Demonstrates a foundational understanding of how AI agents can be applied to enhance and streamline administrative functions
- Knowledge and experience involving the development, management, acquisition and/ or implementation of major communications, computer, command and control, or intelligence (C4I) systems and/ or programmes
- Prior experience of working in an international environment comprising both military and civilian elements
- Knowledge of NATO responsibilities and organization, including Allied Command Operations (ACO) and Allied Command Transformation (ACT)

Language Proficiency:

A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other is desirable.

NOTE: Most of the work of the NCIA is conducted in the English language.

Competencies or Personal Attributes:

Leading and Managing: Provides others with a clear direction; motivates and empowers others; attracts and develops staff of a high calibre; provides staff with development opportunities and coaching; sets appropriate standards of behaviour.

Deciding and Initiating Action: Takes responsibility for actions, projects and people; takes initiative and works under own direction; initiates and generates activity and introduces changes into work processes; makes quick, clear decisions which may include tough choices or considered risks.

Entrepreneurial Thinking: Keeps up to date with best practice and industry trends; identifies business opportunities for the organization; maintains awareness of developments both internally and externally; demonstrates financial awareness; controls costs and thinks in terms of gains, losses and added value.

Adhering to principles & values: Upholds ethics and values; demonstrates integrity; promotes and defends equal opportunities, builds diverse teams; encourages organizational and individual responsibility towards the community and the environment.

Relating & Networking: Easily establishes good relationships with customers and staff; relates well to people at all levels; builds wide and effective networks of contacts; uses humour appropriately to bring warmth to relationships with others

Adapting & responding to change: Adapts to changing circumstances; thrives in conditions of ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people or situations; shows an interest in new experiences.

Formulating strategies & concepts: Works strategically to realise organizational goals; sets and develops strategies; identifies, develops positive and compelling visions of the organization's future; takes account of a wide range of issues across, and related to, the organization.