CAREER PATHWAY EXECUTIVE CYBER LEADERSHIP (901)

January 2021

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

CIO COUNCIL

CHCO COUNCIL

Table of Contents

1 901-EXECUTIVE CYBER LEADERSHIP

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 901-Executive Cyber Leadership.

Table 1. 901-Executive Cyber Leadership Work Role Overview

NICE Role Description	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.
OPM Occupational Series	Personnel performing the 901-Executive Cyber Leadership work role are most commonly aligned to the following Occupational Series: (Top 5 Shown) - 2210-Information Technology Management – 48% - 1811-Criminal Investigation – 20% - 0340-Program Management – 9% - 0301-Miscellaneous Administration and Program – 6% - 0132-Intelligence – 2%
Work Role Pairings	Personnel performing the 901-Executive Cyber Leadership work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 801-Program Manager – 16% - 752-Cyber Policy and Strategy Planner – 13% - 611-Authorizing Official/Designating Rep – 12% - 751-Cyber Workforce Developer and Manager – 8% - 804-IT Investment/Portfolio Manager – 5%
Functional Titles	Personnel performing the 901-Executive Cyber Leadership work role may unofficially or alternatively be called: - Chief Executive Officer (CEO) - Chief Information Security Officer (CISO) - Chief Security Officer (CSO) - Chief Technology Officer (CTO) - Enterprise Risk Manager - Head of Agency / Organization - Senior Agency Information Security Officer (SAISO) - Senior Agency Officials
Distribution of GS-Levels	Personnel performing the 901-Executive Cyber Leadership work role are most commonly found within the following grades on the General Schedule.*

	- ☒ GS-11 – redacted** - ☒ GS-12 – 6% - ☒ GS-13 – 8% - ☒ GS-14 – 20% - ☒ GS-15 – 26% *40% of all 901s are in non-GS pay plans and excluded from this section *Percentages less than 3% have been redacted
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 901-Executive Cyber Leadership work role: - 611-Authorizing Official/Designating Representative - 651-Enterprise Architect - 652-Security Architect - 722-Information Systems Security Manager - 731-Cyber Legal Advisor - 752-Cyber Policy and Strategy Planner - 801-Program Manager - 804-IT Investment/Portfolio Manager - 805-IT Program Auditor
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 901-Executive Cyber Leadership work role. This is not an exhaustive list, nor does it consider learning and development opportunities an individual may pursue to prepare themselves for performing alternate work roles: - 611-Authorizing Official/Designating Representative

1.2 Core Tasks

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 901-Executive Cyber Leadership work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 901-Executive Cyber Leadership Core Tasks

Task ID	Task Description	Core (C) or Additional (A)
T0001	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	N/A*
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	N/A*
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	N/A*
T0006	Advocate organization's official position in legal and legislative proceedings.	N/A*
T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	N/A*
T0066	Develop and maintain strategic plans.	N/A*
T0130	Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.	N/A*
T0134	Lead and align information technology (IT) security priorities with the security strategy.	N/A*
T0135	Lead and oversee information security budget, staffing, and contracting.	N/A*
T0148	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	N/A*
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	N/A*
T0227	Recommend policy and coordinate review and approval.	N/A*
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	N/A*
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	N/A*
T0248	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	N/A*
T0254	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	N/A*
T0263	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.	N/A*
T0264	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	N/A*
T0282	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	N/A*

Task ID	Task Description	Core (C) or Additional (A)
T0337	Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.	N/A*
T0356	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	N/A*
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	N/A*
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	N/A*
T0509	Perform an information security risk assessment.	N/A*
T0763	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	N/A*
T0871	Collaborate on cyber privacy and security policies and procedures	N/A*
T0872	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation	N/A*
T0927	Appoint and guide a team of IT security experts.	N/A*

**Task criticality was not assessed for the 901-Executive Cyber Leadership work role. Core task designation is unavailable at this time.*

1.3 CORE KNOWLEDGE, SKILLS, AND ABILITIES

The table below provides a ranking of KSAs that represent the Core, or baseline, expectations for performance in the 901-Executive Cyber Leadership work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 901-Executive Cyber Leadership Core KSAs

KSA ID	Description	Competency	Importance to Work Role
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to all Work Roles
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to all Work Roles
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence	Foundational to all Work Roles
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security	Foundational to all Work Roles
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to all Work Roles
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to all Work Roles
A0130	Ability to ensure that senior officials within the organization provide information security for the information and systems that support the operations and assets under their control.	Asset / Inventory Management	N/A*
S0359	Skill to use critical thinking to analyze organizational patterns and relationships.	Critical Thinking	N/A*
S0359	Skill to use critical thinking to analyze organizational patterns and relationships.	Critical Thinking	N/A*
A0070	Ability to apply critical reading/thinking skills.	Critical Thinking	N/A*
A0085	Ability to exercise judgment when policies are not well-defined.	Critical Thinking	N/A*
A0106	Ability to think critically.	Critical Thinking	N/A*
A0105	Ability to tailor technical and planning information to a customer's level of understanding.	Information Management	N/A*
K0296	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	Infrastructure Design	N/A*

KSA ID	Description	Competency	Importance to Work Role
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	Interpersonal Skills	N/A*
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	Interpersonal Skills	N/A*
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	Legal, Government, and Jurisprudence	N/A*
A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.	Organizational Awareness	N/A*
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.	Organizational Awareness	N/A*
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	Organizational Awareness	N/A*
S0018	Skill in creating policies that reflect system security objectives.	Policy Management	N/A*
S0018	Skill in creating policies that reflect system security objectives.	Policy Management	N/A*
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management	N/A*
A0116	Ability to prioritize and allocate cybersecurity resources correctly and efficiently.	Strategic Planning	N/A*
A0129	Ability to ensure information security management processes are integrated with strategic and operational planning processes.	Strategic Planning	N/A*
K0628	Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.	Teaching Others	N/A*
S0358	Skill to remain aware of evolving technical infrastructures.	Technology Awareness	N/A*
S0358	Skill to remain aware of evolving technical infrastructures.	Technology Awareness	N/A*
S0357	Skill to anticipate new security threats.	Threat Analysis	N/A*
S0357	Skill to anticipate new security threats.	Threat Analysis	N/A*

KSA ID	Description	Competency	Importance to Work Role
K0009	Knowledge of application vulnerabilities.	Vulnerabilities Assessment	N/A*
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment	N/A*
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment	N/A*
K0314	Knowledge of industry technologies' potential cybersecurity vulnerabilities.	Vulnerabilities Assessment	N/A*
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	Vulnerabilities Assessment	N/A*
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	N/A*

**Knowledge, Skill, and Ability criticality was not assessed for the 901-Executive Cyber Leadership work role. Core KSA designation is unavailable at this time.*

1.4 Core Competencies

The table below is a compilation of competencies aligned to the 901-Executive Cyber Leadership work role, and their associated importance. Listed competencies are collections of three or more similar Knowledge, Skills, or Abilities aligned to the Work Role. *These competencies originate from the NICE Framework Competency Pivot Tool*.

Table 4. 901-Executive Cyber Leadership Core Competencies

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Critical Thinking	C011	KSAs that relate to the objective analysis of facts to form a judgment	• Skill to use critical thinking to analyze organizational patterns and relationships. • Skill to use critical thinking to analyze organizational patterns and relationships. • Ability to apply critical reading/thinking skills. • Ability to exercise judgment when policies are not well-defined. • Ability to think critically.	*N/A
Organizational Awareness	C037	KSAs that relate to understanding an organization's mission and functions, its social and political structure and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization.	• Ability to relate strategy, business, and technology in the context of organizational dynamics. • Ability to understand technology, management, and leadership issues related to organization processes and problem solving. • Ability to understand the basic concepts and issues related to cyber and its organizational impact.	N/A*
Policy Management	C038	KSAs that relate to the process of creating, communicating, and maintaining policies and procedures within an organization	• Skill in creating policies that reflect system security objectives. • Skill in creating policies that reflect system security objectives. • Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	N/A*

Technical Competency	Comp . ID	Definition	Work Role Related KSAs	Importance
Vulnerabilities Assessment	C057	KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	• Knowledge of application vulnerabilities. • Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). • Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. • Knowledge of industry technologies' potential cybersecurity vulnerabilities. • Knowledge of emerging security issues, risks, and vulnerabilities. • Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	N/A*

**Competency criticality was not assessed for the 901-Executive Cyber Leadership work role. Core competency designation is unavailable at this time.*

1.5 Suggested Qualifications / Capability Indicators

Table 5. 901-Executive Cyber Leadership Suggested Qualifications

For indicators of capability for the 901-Executive Cyber Leadership work role, please see Draft NISTR 8193 - National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators.

Section to be populated with updated DoD-8140 Qualification Matrix for 901-Executive Cyber Leadership.