CAREER PATHWAY INFORMATION SYSTEMS SECURITY MANAGER (722)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

CIO COUNCIL

CHIEF HUMAN CAPITAL OFFICERS COUNCIL
CHCO COUNCIL
UNITED STATES OF AMERICA

Table of Contents

1 722-INFORMATION SYSTEMS SECURITY MANAGER

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 722-Information Systems Security Manager.

Disclaimer: The 722-Information Systems Security Manager work role contains tasks and knowledge, skills, and abilities that may be shared amongst Information Systems Security Officers (ISSOs) as well as Information Systems Security Managers (ISSMs).

Table 1. 722-Information Systems Security Manager Work Role Overview

NICE Role Description	Responsible for the cybersecurity of a program, organization, system, or enclave.
OPM Occupational Series	Personnel performing the 722-Information Systems Security Manager work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 83% - 0080-Security Administration – 4% - 1550-Computer Science – 3% - 0301-Miscellaneous Administration and Program – 2% - 0343-Management and Program Analysis – 2%
Work Role Pairings	Personnel performing the 722-Information Systems Security Manager work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 612-Security Control Assessor – 19% - 541-Vulnerability Assessment Analyst – 10% - 752-Cyber Policy and Strategy Planner – 10% - 461-Systems Security Analyst – 7% - 723-COMSEC Manager – 6%
Functional Titles	Personnel performing the 722-Information Systems Security Manager work role may unofficially or alternatively be called: - Common Control Provider - Cybersecurity Officer - Enterprise Security Officer - Information Assurance Analyst - Information Assurance Security Manager - Information Assurance Security Officer - Information Security Program Manager - Information Systems Security Officer (ISSO) - Information Systems Security Specialist - Security Domain Specialist
Distribution of GS-Levels	Personnel performing the 722-Information Systems Security Manager work role are most commonly found within the following grades on the General Schedule*.

	- ☐ GS-6 – redacted** - ☐ GS-7 – redacted** - ☐ GS-9 – redacted** - ☐ GS-10 – redacted** - ☒ GS-11 – 9% - ☒ GS-12 – 25% - ☒ GS-13 – 26% - ☒ GS-14 – 16% - ☒ GS-15 – 5% *19% of all personnel performing the 722-Information Systems Security Manager work role are in non-GS pay plans and are 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 722-Information Systems Security Manager work role: - 441-Network Operations Specialist - 671-System Testing and Evaluation Specialist - 461-Systems Security Analyst - 511-Cyber Defense Analyst - 521-Cyber Defense Infrastructure Support Specialist - 531-Cyber Defense Incident Responder - 541-Vulnerability Assessment Analyst - 612-Security Control Assessor - 622-Secure Software Assessor - 723-Communications Security (COMSEC) Manager - 732-Privacy Compliance Manager
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 722-Information Systems Security Manager. 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: - 612-Security Control Assessor - 723-Communications Security (COMSEC) Manager *Note: Leveraging the knowledge, skills, abilities, and tasks of the 722-Information Systems Security Manager work role, individuals may prepare themselves to transition into one or more of the following cross-functional work roles: - *711- Cyber Instructional Curriculum Developer* - *712-Cyber Instructor* - *732-Privacy Compliance Manager / Officer* - *751-Cyber Workforce Developer and Manager* - *752-Cyber Policy and Strategy Planner* - *802-IT Project Manager* - *901-Executive Cyber Leadership*

1.2 Core Tasks

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 722-Information Systems Security Manager work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 722-Information Systems Security Manager Core Tasks

Task ID	Task	Core or Additional
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.	Core
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Core
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.	Core
T0024	Collect and maintain data needed to meet system cybersecurity reporting.	Core
T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Core
T0089	Ensure that security improvement actions are evaluated, validated, and implemented as required.	Core
T0091	Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.	Core
T0092	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	Core
T0097	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.	Core
T0106	Identify alternative information security strategies to address organizational security objective.	Core
T0115	Identify information technology (IT) security program implications of new technologies or technology upgrades.	Core
T0133	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s cybersecurity program.	Core
T0147	Manage the monitoring of information security data sources to maintain organizational situational awareness.	Core
T0157	Oversee the information security training and awareness program.	Core
T0158	Participate in an information security risk assessment during the Security Assessment and Authorization process.	Core
T0159	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	Core
T0192	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.	Core
T0211	Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	Core

Task ID	Task	Core or Additional
T0215	Recognize a possible security violation and take appropriate action to report the incident, as required.	Core
T0219	Recommend resource allocations required to securely operate and maintain an organization’s cybersecurity requirements.	Core
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Core
T0234	Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.	Core
T0248	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Core
T0254	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	Core
T0263	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.	Core
T0264	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Core
T0265	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.	Core
T0275	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Core
T0280	Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.	Core
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	Additional
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Additional
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Additional
T0093	Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.	Additional
T0095	Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy.	Additional
T0099	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Additional
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.	Additional
T0132	Interpret and/or approve security requirements relative to the capabilities of new information technologies.	Additional
T0134	Lead and align information technology (IT) security priorities with the security strategy.	Additional

Task ID	Task	Core or Additional
T0135	Lead and oversee information security budget, staffing, and contracting.	Additional
T0148	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	Additional
T0149	Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.	Additional
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	Additional
T0199	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Additional
T0206	Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.	Additional
T0213	Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.	Additional
T0227	Recommend policy and coordinate review and approval.	Additional
T0239	Use federal and organization-specific published documents to manage operations of their computing environment system(s).	Additional
T0255	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.	Additional
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Additional
T0276	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.	Additional
T0277	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Additional
T0281	Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary.	Additional
T0282	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Additional

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 722-Information Systems Security Manager work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 722-Information Systems Security Manager Core Knowledge, Skills, and Abilities

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security	Foundational to All Work Roles
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	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
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to All Work Roles
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to All Work Roles
K0021	Knowledge of data backup and recovery.	Business Continuity	Core
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.	Business Continuity	Core
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense	Core
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration	Core
K0018	Knowledge of encryption algorithms	Encryption	Core
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture	Core
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Core
K0053	Knowledge of measures or indicators of system performance and availability.	Information Technology Assessment	Core
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence	Core
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence	Core
K0058	Knowledge of network traffic analysis methods.	Network Management	Core
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management	Core

KSA ID	Description	Competency	Importance to Work Role
K0077	Knowledge of server and client operating systems.	Operating Systems	Core
S0018	Skill in creating policies that reflect system security objectives.	Policy Management	Core
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management	Core
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness	Core
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis	Core
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment	Core
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	Core
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment	Core
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment	Core
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture	Additional
K0042	Knowledge of incident response and handling methodologies.	Incident Management	Additional
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management	Additional
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance	Additional
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance	Additional
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security	Additional
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment	Additional
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment	Additional

KSA ID	Description	Competency	Importance to Work Role
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design	Additional
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design	Additional
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design	Additional
K0072	Knowledge of resource management principles and techniques.	Project Management	Additional
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management	Additional
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis	Additional
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management	Additional
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management	Additional
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration	Additional
K0076	Knowledge of server administration and systems engineering theories, concepts, and methods.	Systems Integration	Additional
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	Systems Integration	Additional
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration	Additional
K0092	Knowledge of technology integration processes.	Systems Integration	Additional
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.	Third Party Oversight/Acquisition Management	Additional
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Additional
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional
A0128	Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.	Computer Network Defense	Additional
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement	Additional
K0163	Knowledge of critical information technology (IT) procurement requirements.	Contracting/Procurement	Additional

KSA ID	Description	Competency	Importance to Work Role
A0161	Ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).	Contracting/Procurement	Additional
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis	Additional
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Additional
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Data Privacy and Protection	Additional
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection	Additional
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 722-Information Systems Security Manager 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. 722-Information Systems Security Manager Core Competencies

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Contracting / Procurement	C010	KSAs that relate to the various types of contracts, techniques for contracting or procurement, and contract negotiation and administration.	- Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161) - Knowledge of critical information technology (IT) procurement requirements. - Ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).	Core
Data Privacy and Protection	C014	KSAs that relate to the relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them	- Knowledge of Personally Identifiable Information (PII) data security standards. - Knowledge of Payment Card Industry (PCI) data security standards. - Knowledge of Personal Health Information (PHI) data security standards.	Core
Information Technology Assessment	C025	KSAs that relate to the principles, methods, and tools (for example, surveys, system performance measures) to assess the effectiveness and practicality of information technology systems.	- Knowledge of measures or indicators of system performance and availability. - Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. - Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Core
Legal Government and Jurisprudence	C030	KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.	- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. - Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. - Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Risk Management	C044	KSAs that relate to the methods and tools used for risk assessment and mitigation of risk.	- Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). - Knowledge of Risk Management Framework (RMF) requirements. - Knowledge of organization's risk tolerance and/or risk management approach. - Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Core
Systems Integration	C049	KSAs that relate to the principles, methods, and procedures for installing, integrating, and optimizing information systems components.	- Knowledge of server administration and systems engineering theories, concepts, and methods. - Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design. - Knowledge of system life cycle management principles, including software security and usability. - Knowledge of technology integration processes.	Core
Vulnerabilities Assessment	C057	KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	- Knowledge of cyber threats and vulnerabilities. - Knowledge of specific operational impacts of cybersecurity lapses. - Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). - 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 penetration testing principles, tools, and techniques. - Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Infrastructure Design	C026	KSAs that relate to the architecture and typology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.	- Knowledge of computer networking concepts and protocols, and network security methodologies. - Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). - Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Additional
Information Systems / Network Security	C024	KSAs that relate to the methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore security of information systems and network services.	- Knowledge of cybersecurity and privacy principles. - Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists). - Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 722-Information Systems Security Manager Suggested Qualifications / Capability Indicators

For indicators of capability for the 722-Information Systems Security Manager 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 722-Information Systems Security Manager.

2 APPENDIX: 722-INFORMATION SYSTEMS SECURITY MANAGER TASK ANALYSIS AND KSA MAPPING

2.1 KEY TO READING THE TASK ANALYSIS AND KSA MAPPING

Table 6. Key to Reading the Task Analysis and KSA Mapping

Proficiency	Task Statement	Importance
As Written	Task as written within the NICE Cybersecurity Workforce Framework (NICE Framework).	Overall Importance to Work Role
Entry	*Example behavioral indicator / task permutation for performing this task at an Entry skills proficiency level.*	
Intermediate	*Example behavioral indicator / task permutation for performing this task at an Intermediate skills proficiency level.*	
Advanced	*Example behavioral indicator / task permutation for performing this task at an Advanced skills proficiency level.*	

Table 7. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
ID of K, S, or A	Knowledge, Skill or Ability needed to perform the task as written within the NICE Framework	Competency mapped to the individual K, S, or A.

2.2 722-Information Systems Security Manager Task Analysis and KSA Mapping

Table 8. T0001 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	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.	Core
Entry	*Research and recommend necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall system / program risk.*	
Intermediate	*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.*	
Advanced	*Evaluate the effectiveness of the necessary resources, including leadership support, financial resources, and key security personnel, to improve the effectiveness of information technology (IT) security goals and objectives and reduce overall organizational risk.*	

Table 9. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management

KSA ID	Description	Competency
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
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
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement
K0163	Knowledge of critical information technology (IT) procurement requirements.	Contracting/Procurement
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0053	Knowledge of measures or indicators of system performance and availability.	Information Technology Assessment
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 10. T0003 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Advise senior management (e.g., CIO) on risk levels and security posture.	Core
Entry	*Communicate risk levels and security posture.*	
Intermediate	*Consult with supervisors on risk levels and security posture and how to reduce risk.*	
Advanced	*Advise senior management on risk levels and security posture and provide recommendations for risk reduction*	

Table 11. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0077	Knowledge of server and client operating systems.	Operating Systems
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense

Table 12. T0005 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.	Core
Entry	*Monitor and report changes affecting the organization's cybersecurity posture to appropriate senior leadership.*	
Intermediate	*Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture [and if necessary, make recommendations to correct deficiencies.*	
Advanced	*Advise senior leadership or Authorizing Official of major changes affecting the organization's cybersecurity posture and, if necessary, make recommendations to correct deficiencies.*	

Table 13. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0077	Knowledge of server and client operating systems.	Operating Systems
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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

Table 14. T0265 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.	Core
Entry	*Verify and document successful implementation and functionality of baseline security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.*	
Intermediate	*Review documentation and assure successful implementation and functionality of [tailored] security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.*	
Advanced	*Manage and recommend improvements of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.*	

Table 15. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.	Business Continuity
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
A0161	Ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).	Contracting/Procurement
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management

KSA ID	Description	Competency
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0077	Knowledge of server and client operating systems.	Operating Systems
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
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

Table 16. T0024 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Collect and maintain data needed to meet system cybersecurity reporting.	Core
Entry	*Assist with collecting and maintaining data needed to meet system cybersecurity reporting.*	
Intermediate	*Collect and maintain data needed to meet system cybersecurity reporting.*	
Advanced	*Evaluate data needed to meet system cybersecurity reporting.*	

Table 17. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0053	Knowledge of measures or indicators of system performance and availability.	Information Technology Assessment
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0077	Knowledge of server and client operating systems.	Operating Systems
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis

KSA ID	Description	Competency
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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

Table 18. T0025 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Core
Entry	*Assists with communicating the value of information technology (IT) security.*	
Intermediate	*Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.*	
Advanced	*Advocate the value of information technology (IT) security throughout all levels of the organization stakeholders.*	

Table 19. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0053	Knowledge of measures or indicators of system performance and availability.	Information Technology Assessment
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management

Table 20. T0280 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.	Core
Entry	*Assist with validating the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.*	
Intermediate	*Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.*	
Advanced	*Develop new measures to validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.*	

Table 21. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
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

Table 22. T0264 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Core
Entry	*Develop plans of actions and milestones or remediation plans for vulnerabilities identified during risk assessments, audits, inspections, etc.*	
Intermediate	*Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. Then validate that the plan will remediate the risk.*	
Advanced	*Manage plans of actions and milestones or remediation plans across the organization for vulnerabilities identified during risk assessments, audits, inspections, etc.*	

Table 23. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0077	Knowledge of server and client operating systems.	Operating Systems
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0072	Knowledge of resource management principles and techniques.	Project Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration

KSA ID	Description	Competency
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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

Table 24. T0089 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure security improvement actions are evaluated, validated, and implemented as required.	Core
Entry	*Support efforts to ensure security improvement actions are evaluated, validated, and implemented as required.*	
Intermediate	*Ensure security improvement actions are evaluated, validated, and implemented as required.*	
Advanced	*Lead others to ensure that security improvement actions are evaluated, validated, and implemented as required.*	

Table 25. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0053	Knowledge of measures or indicators of system performance and availability.	Information Technology Assessment
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
K0077	Knowledge of server and client operating systems.	Operating Systems
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management

KSA ID	Description	Competency
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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

Table 26. T0091 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.	Core
Entry	*Assist with coordination and documentation to ensure cybersecurity inspections, tests, and reviews are conducted on the network environment.*	
Intermediate	*Coordinate and document to ensure cybersecurity inspections, tests, and reviews are conducted on the network environment.*	
Advanced	*Coordinate multiple ongoing cybersecurity inspections, tests, and reviews are conducted for the network environment.*	

Table 27. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.	Business Continuity
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management

KSA ID	Description	Competency
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment

Table 28. T0092 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	Core
Entry	*Assist with ensuring that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).*	
Intermediate	*Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).*	
Advanced	*Verify that cybersecurity requirements are integrated into the organizational business continuity planning, make recommendations for improvements on continuity planning.*	

Table 29. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0021	Knowledge of data backup and recovery.	Business Continuity
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.	Business Continuity
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management

Table 30. T0097 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.	Core
Entry	*Ensure baseline security safeguards are appropriately installed.*	
Intermediate	*Ensure and document variances to confirm that baseline security safeguards are appropriately installed.*	
Advanced	*Manage development of tailored baseline security safeguards.*	

Table 31. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
A0161	Ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).	Contracting/Procurement
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0077	Knowledge of server and client operating systems.	Operating Systems
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration

KSA ID	Description	Competency
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	Systems Integration
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0092	Knowledge of technology integration processes.	Systems Integration
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 32. T0106 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify alternative information security strategies to address organizational security objective.	Core
Entry	*Assist with identifying alternative information security strategies to address organizational security objectives.*	
Intermediate	*Identify alternative information security strategies to address organizational security objectives.*	
Advanced	*Develop, review, and approve alternative information security strategies to address organizational security objectives.*	

Table 33. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration

KSA ID	Description	Competency
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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

Table 34. T0115 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify information technology (IT) security program implications of new technologies or technology upgrades.	Core
Entry	*Assist with identifying information technology (IT) security program implications of new technologies or technology upgrades.*	
Intermediate	*Identify and document information technology (IT) security program implications of new technologies or technology upgrades.*	
Advanced	*Advise on the information technology (IT) security program implications of new technologies or technology upgrades and provide recommendations for improving the organizational security posture.*	

Table 35. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
A0161	Ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).	Contracting/Procurement
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0077	Knowledge of server and client operating systems.	Operating Systems
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis

KSA ID	Description	Competency
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	Systems Integration
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
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

Table 36. T0263 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify security requirements specific to an information technology (IT) system in all phases of the System Life Cycle.	Core
Entry	*Demonstrate knowledge of security requirements specific to an information technology (IT) system in all phases of the system life cycle.*	
Intermediate	*Identify security requirements specific to an information technology (IT) system in all phases of the System Life Cycle.*	
Advanced	*Assess security requirements specific to an information technology (IT) system in all phases of the system life cycle.*	

Table 37. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0163	Knowledge of critical information technology (IT) procurement requirements.	Contracting/Procurement
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
K0077	Knowledge of server and client operating systems.	Operating Systems
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	Systems Integration
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis

Table 38. T0133 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	Core
Entry	*Assist with identifying patterns of noncompliance to evaluate their impact on levels of risk and/or overall effectiveness of the organization's cybersecurity program.*	
Intermediate	*Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the organization's cybersecurity program.*	
Advanced	*Interpret patterns of noncompliance to evaluate their impact on levels of risk and make recommendation to improve overall effectiveness of the organization's cybersecurity program.*	

Table 39. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration

KSA ID	Description	Competency
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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

Table 40. T00147 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Manage the monitoring of information security data sources to maintain organizational situational awareness.	Core
Entry	*Assist with the identifying and monitoring of information security data sources to maintain organizational situational awareness.*	
Intermediate	*Identify and monitor information security data sources to maintain organizational situational awareness.*	
Advanced	*Advise others on monitoring methodologies of information security data sources to maintain organizational situational awareness.*	

Table 41. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured	Vulnerabilities Assessment

KSA ID	Description	Competency
	Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	
K0342	Knowledge of penetration testing principles, tools, and techniques.	

Table 42. T0254 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	Core
Entry	*Apply policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.*	
Intermediate	*Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.*	
Advanced	*Develop & implement policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies making recommendations for improvements where appropriate.*	

Table 43. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0163	Knowledge of critical information technology (IT) procurement requirements.	Contracting/Procurement
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management

KSA ID	Description	Competency
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment

Table 44. T0157 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Oversee the information security training and awareness program.	Core
Entry	*Coordinate activities and provide logistics support for the information security training and awareness program.*	
Intermediate	*Develop content and aid in information security training and awareness program implementation.*	
Advanced	*Advocate and advise on resources to support the information security training and awareness program.*	

Table 45. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis

KSA ID	Description	Competency
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 46. T0158 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Participate in an information security risk assessment during the Security Assessment and Authorization process.	Core
Entry	*Assist others and gather information in an information security risk assessment in preparation for and during the Security Assessment and Authorization process.*	
Intermediate	*Participate in and provide input during information security risk assessments in preparation for and during the Security Assessment and Authorization process.*	
Advanced	*Oversee systems and organizational progress for information security risk assessments during the Security Assessment and Authorization process.*	

Table 47. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration

KSA ID	Description	Competency
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment

Table 48. T0159 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	Core
Entry	*Work with others in the development or modification of the computer environment cybersecurity program plans and requirements.*	
Intermediate	*Develop or modify the computer environment cybersecurity program plans and requirements.*	
Advanced	*Review, approve, and provide further recommendations to the development or modification of the computer environment cybersecurity program plans and requirements.*	

Table 49. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis

Table 50. T00192 *Task Analysis*

Proficiency	Task Statement	Importance
As Written within Framework	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.	Core
Entry	*Assists in the preparation, distribution, and maintenance of plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.*	
Intermediate	*Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.*	
Advanced	*Review and recommend changes or approval for plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.*	

Table 51. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management

Table 52. T0248 *Task Analysis*

Proficiency	Task Statement	Importance
As Written within Framework	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Core
Entry	*Assist with promoting awareness of how security issues are reflected in and affected by the organization's vision and goals.*	
Intermediate	*Research and communicate security issues that are affected by the organization's vision and goals.*	
Advanced	*Assist in the development of organization's vision and goals that promote good security policies and practices.*	

Table 53. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0053	Knowledge of measures or indicators of system performance and availability.	Information Technology Assessment
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis

Table 54. T0211 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provide system related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	Core
Entry	Assist with providing system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	
Intermediate	Provide system related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	
Advanced	Evaluate system-related input on cybersecurity requirements and recommend improvements where appropriate, to be included in statements of work and other appropriate procurement documents.	

Table 55. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement
K0163	Knowledge of critical information technology (IT) procurement requirements.	Contracting/Procurement
A0161	Ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).	Contracting/Procurement
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management

KSA ID	Description	Competency
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management

Table 56. T0215 *Task Analysis*

Proficiency	Task Statement	Importance
As Written within Framework	Recognize a possible security violation and take appropriate action to report the incident, as required.	Core
Entry	*Recognize and assess a possible security violation and take appropriate action to report the incident, as required.*	
Intermediate	*Lead a response team in investigating possible security violations and take appropriate action to report and remediate the incident, as required.*	
Advanced	*Develop policies and procedures to address security violations within your organization.*	

Table 57. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment

Table 58. T0219 *Task Analysis*

Proficiency	Task Statement	Importance
As Written within Framework	Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.	Core
Entry	*Assess resource allocations required to securely operate and maintain an organization's cybersecurity requirements and determine if those resources are adequate.*	
Intermediate	*Develop and write resource allocation requirements to securely operate and maintain an organization's cybersecurity requirements.*	
Advanced	*Review and recommend/approve resource allocations required to securely operate and maintain an organization's cybersecurity requirements.*	

Table 59. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0053	Knowledge of measures or indicators of system performance and availability.	Information Technology Assessment
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0077	Knowledge of server and client operating systems.	Operating Systems
K0072	Knowledge of resource management principles and techniques.	Project Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management

KSA ID	Description	Competency
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
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

Table 60. T0229 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Core
Entry	*Assist with ensuring protective or corrective measures are implemented when a cybersecurity incident or vulnerability is discovered.*	
Intermediate	*Develop and ensure protective or corrective measures are implemented when a cybersecurity incident or vulnerability is discovered.*	
Advanced	*Supervise and manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered and, when necessary, communicate impact of implemented protective or corrective measures to appropriate stakeholders (e.g. System Owners, Leadership).*	

Table 61. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 62. T0275 *Task Analysis*

Proficiency	Task Statement	Importance
As Written within Framework	Support necessary compliance activities (e.g., ensure system security configuration guidelines are followed, compliance monitoring occurs).	Core
Entry	*Assist in compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).*	
Intermediate	*Support and provide input for necessary compliance activities (e.g., ensure system security configuration guidelines are followed, compliance monitoring occurs).*	
Advanced	*Evaluate and provide corrective actions for necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).*	

Table 63. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0077	Knowledge of server and client operating systems.	Operating Systems
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis

KSA ID	Description	Competency
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0076	Knowledge of server administration and systems engineering theories, concepts, and methods.	Systems Integration
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	Systems Integration
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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

Table 64. T0234 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Track audit findings and recommendations to ensure appropriate mitigation actions are taken.	Core
Entry	*Assist with tracking audit findings and recommendations to ensure appropriate mitigation actions are taken.*	
Intermediate	*Independently track audit findings and recommendations to ensure appropriate mitigation actions are taken.*	
Advanced	*Review team efforts to track audit findings and recommendations and approve appropriate mitigation actions.*	

Table 65. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration
K0101	Knowledge of the organization’s enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Incident Management
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
S0018	Skill in creating policies that reflect system security objectives.	Policy Management
K0072	Knowledge of resource management principles and techniques.	Project Management
K0121	Knowledge of information security program management and project management principles and techniques.	Project Management
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	Risk Management

KSA ID	Description	Competency
K0167	Knowledge of system administration, network, and operating system hardening techniques.	System Administration
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0151	Knowledge of current and emerging threats/threat vectors.	Threat Analysis
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
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
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment