CAREER PATHWAY INFORMATION SYSTEMS SECURITY DEVELOPER (631)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 631-INFORMATION SYSTEMS SECURITY DEVELOPER

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 631-Information Systems Security Developer.

Table 1. 631-Information Systems Security Developer Work Role Overview

NICE Role Description	Designs, develops, tests, and evaluates information security throughout the systems development life cycle.
OPM Occupational Series	Personnel performing the 631-Information Systems Security Developer work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 66% - 0855-Electronics Engineering – 11% - 1550-Computer Science – 8% - 0854-Computer Engineering – 8% - 0801-General Engineering – 2%
Work Role Pairings	Personnel performing the 631-Information Systems Security Developer work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 651-Systems Requirements Planner – 14% - 632-Systems Developer – 13% - 451-System Administrator – 13% - 461-Systems Security Analyst – 8% - 722-Information Systems Security Manager – 8%
Functional Titles	Personnel performing the 631-Information Systems Security Developer work role may unofficially or alternatively be called: - Information Assurance (IA) Developer - Information Assurance Engineer - Information Systems Security Engineer - Security / Systems Engineer - Telecommunications Engineer
Distribution of GS-Levels	Personnel performing the 631-Information Systems Security Developer work role are most commonly found within the following grades on the General Schedule*. - ☐ GS-4 – redacted** - ☐ GS-7 – redacted** - ☐ GS-9 – redacted** - ☒ GS-11 – 4%

	- ☒ GS-12 – 12% - ☒ GS-13 – 19% - ☒ GS-14 – 19% - ☒ GS-15 – 5% *42% of all 651s are in non-GS pay plans and excluded from this section **Percentages less than 3% have been redacted
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 631-Information Systems Security Developer work role: - 632-Systems Developer - 661-Research and Development Specialist
Off Ramps	The following work roles are examples of possible roles an individual may transition to after having performed the 631-Information Systems Security Developer work role: - 651-Enterprise Architect - 652-Security Architect *Note: Leveraging the knowledge, skills, abilities, and tasks of the 631-Information Systems Security Developer 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*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 631-Information Systems Security Developer work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 631-Information Systems Security Developer Core Tasks

Task ID	Task	Core or Additional
T0012	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.	Core
T0015	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Core
T0018	Assess the effectiveness of cybersecurity measures utilized by system(s).	Core
T0019	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	Core
T0021	Build, test, and modify product prototypes using working models or theoretical models.	Core
T0032	Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Core
T0053	Design and develop cybersecurity or cybersecurity-enabled products.	Core
T0055	Design hardware, operating systems, and software applications to adequately address cybersecurity requirements.	Core
T0056	Design or integrate appropriate data backup capabilities into overall system designs and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Core
T0061	Develop and direct system testing and validation procedures and documentation.	Core
T0069	Develop detailed security design documentation for component and interface specifications to support system design and development.	Core
T0070	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Core
T0076	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.	Core
T0107	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find workarounds for communication protocols that are not interoperable).	Core
T0122	Implement security designs for new or existing system(s).	Core
T0124	Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).	Core
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Core

Task ID	Task	Core or Additional
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Core
T0228	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Core
T0231	Provide support to security/certification test and evaluation activities.	Core
T0269	Design and develop key management functions (as related to cybersecurity).	Core
T0270	Analyze user needs and requirements to plan and conduct system security development.	Core
T0272	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	Core
T0304	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	Core
T0326	Employ configuration management processes.	Core
T0359	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	Core
T0446	Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.	Core
T0449	Design to security requirements to ensure requirements are met for all systems and/or applications.	Core
T0509	Perform an information security risk assessment.	Core
T0518	Perform security reviews and identify security gaps in architecture.	Core
T0078	Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.	Additional
T0105	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.	Additional
T0109	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.	Additional
T0119	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements.	Additional
T0201	Provide guidelines for implementing developed systems to customers or installation teams.	Additional
T0242	Utilize models and simulations to analyze or predict system performance under different operating conditions.	Additional
T0271	Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity	Additional

Task ID	Task	Core or Additional
	and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	
T0466	Develop mitigation strategies to address cost, schedule, performance, and security risks.	Additional
T0527	Provide input to implementation plans and standard operating procedures as they relate to information systems security.	Additional
T0541	Trace system requirements to design components and perform gap analysis.	Additional
T0544	Verify stability, interoperability, portability, and/or scalability of system architecture.	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 631-Information Systems Security Developer work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 631-Information Systems Security Developer 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
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to All Work Roles
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to All Work Roles
K0032	Knowledge of resiliency and redundancy.	Business Continuity	Core
S0023	Skill in designing security controls based on cybersecurity principles and tenets.	Computer Network Defense	Core
K0024	Knowledge of database systems.	Database Management Systems	Core
K0018	Knowledge of encryption algorithms	Encryption	Core
K0308	Knowledge of cryptology.	Encryption	Core
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture	Core
K0067	Knowledge of process engineering concepts.	Enterprise Architecture	Core
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture	Core
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).	Identity Management	Core
K0065	Knowledge of policy-based and risk adaptive access controls.	Identity Management	Core
K0336	Knowledge of access authentication methods.	Identity Management	Core
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance	Core

KSA ID	Description	Competency	Importance to Work Role
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Core
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance	Core
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security	Core
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security	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
K0276	Knowledge of security management.	Information Systems/Network Security	Core
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security	Core
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment	Core
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design	Core
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	Core
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design	Core
K0322	Knowledge of embedded systems.	Infrastructure Design	Core
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design	Core
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design	Core
K0015	Knowledge of computer algorithms.	Mathematical Reasoning	Core
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management	Core
K0060	Knowledge of operating systems.	Operating Systems	Core
K0084	Knowledge of structured analysis principles and methods.	Risk Management	Core

KSA ID	Description	Competency	Importance to Work Role
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development	Core
K0082	Knowledge of software engineering.	Software Development	Core
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration	Core
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration	Core
K0036	Knowledge of human-computer interaction principles.	Systems Integration	Core
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration	Core
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	Core
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration	Core
K0102	Knowledge of the systems engineering process.	Systems Integration	Core
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation	Core
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis	Core
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment	Core
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment	Core
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages	Additional
K0030	Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).	Computers and Electronics	Additional
K0055	Knowledge of microprocessors.	Computers and Electronics	Additional
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement	Additional
A0056	Ability to ensure security practices are followed throughout the acquisition process.	Contracting/Procurement	Additional
A0108	Ability to understand objectives and effects.	Critical Thinking	Additional
K0066	Knowledge of Privacy Impact Assessments.	Data Privacy and Protection	Additional
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Additional

KSA ID	Description	Competency	Importance to Work Role
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
A0008	Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).	Enterprise Architecture	Additional
A0061	Ability to design architectures and frameworks.	Enterprise Architecture	Additional
S0031	Skill in developing and applying security system access controls.	Identity Management	Additional
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management	Additional
A0048	Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Additional
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment	Additional
A0074	Ability to collaborate effectively with others.	Interpersonal Skills	Additional
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—to leverage analytical and technical expertise.	Interpersonal Skills	Additional
A0098	Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.	Interpersonal Skills	Additional
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).	Mathematical Reasoning	Additional
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	Mathematical Reasoning	Additional
S0160	Skill in the use of design modeling (e.g., unified modeling language).	Modeling and Simulation	Additional
A0012	Ability to ask clarifying questions.	Oral Communication	Additional

KSA ID	Description	Competency	Importance to Work Role
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	Organizational Awareness	Additional
S0145	Skill in integrating and applying policies that meet system security objectives.	Policy Management	Additional
A0013	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	Presenting Effectively	Additional
A0040	Ability to translate data and test results into evaluative conclusions.	Problem Solving	Additional
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management	Additional
A0049	Ability to apply secure system design tools, methods and techniques.	System Administration	Additional
A0050	Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools.	System Administration	Additional
S0024	Skill in designing the integration of hardware and software solutions.	Systems Integration	Additional
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation	Additional
A0026	Ability to analyze test data.	Systems Testing and Evaluation	Additional
K0093	Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).	Telecommunications	Additional
K0297	Knowledge of countermeasure design for identified security risks.	Threat Analysis	Additional
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment	Additional
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment	Additional
A0019	Ability to produce technical documentation.	Written Communication	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 631-Information Systems Security Developer 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. 631-Information Systems Security Developer Core Competencies

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Enterprise Architecture	C018	KSAs that relate to the principles, concepts, and methods of enterprise architecture to align information technology (IT) strategy, plans, and systems with the mission, goals, structure, and processes of the organization.	- Knowledge of parallel and distributed computing concepts. - Knowledge of process engineering concepts. - Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]). - Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]). - Ability to design architectures and frameworks.	Core
Identity Management	C020	KSAs that relate to the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons"	- Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML). - Knowledge of policy-based and risk adaptive access controls. - Knowledge of access authentication methods. - Skill in developing and applying security system access controls.	Core
Information Assurance	C022	KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	- Knowledge of organization's enterprise information security architecture. - Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). - Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). - Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). - Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
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 information security systems engineering principles (NIST SP 800-160). - Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). - Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). - Knowledge of security management. - Skill in discerning the protection needs (i.e., security controls) of information systems and networks. - Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Core
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 local area and wide area networking principles and concepts including bandwidth management. - 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 embedded systems. - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. - Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Core
System Administration	C048	KSAs that relate to the upkeep, configuration, and reliable operation of computer systems.	- Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org). - Ability to apply secure system design tools, methods and techniques. - Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools.	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Systems Testing and Evaluation	C050	KSAs that relate to the principles, methods, and tools for analyzing and administering systems test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.	- Knowledge of systems testing and evaluation methods. - Knowledge of organization's evaluation and validation requirements. - Ability to analyze test data.	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. - Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. - Skill in evaluating the adequacy of security designs. - Ability to identify systemic security issues based on the analysis of vulnerability and configuration data. - Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	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 Privacy Impact Assessments. - 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.	Additional
Mathematical Reasoning	C031	KSAs that relate to devising strategies to solve a wide variety of math problems and determine if an assertion is correct.	- Knowledge of computer algorithms. - Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis). - Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	Additional
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 structured analysis principles and methods. - Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 631-Information Systems Security Developer Suggested Qualifications / Capability Indicators

For indicators of capability for the 631-Information Systems Security Developer 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 631-Information Systems Security Developer.

2 APPENDIX: 631-INFORMATION SYSTEMS SECURITY DEVELOPER 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.

2.2 631-INFORMATION SYSTEMS SECURITY DEVELOPER TASK ANALYSIS AND KSA MAPPING

Table 8. T0012 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.	Core
Entry	*Gather information on potential design constraints to identify trade-offs and detailed system and security design, and consider life cycle support, and assist with remediation efforts.*	
Intermediate	*Analyze and remediate design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.*	
Advanced	*Lead and remediate complex design constraints and manage trade-offs, detailed system and security design, and life cycle support.*	

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

KSA ID	Description	Competency
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	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
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	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

KSA ID	Description	Competency
K0102	Knowledge of the systems engineering process.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 10. T0015 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Core
Entry	*Catalogue security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.*	
Intermediate	*Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.*	
Advanced	*Develop security policies for applications that interface with one another, such as Business-to-Business (B2B) applications.*	

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

KSA ID	Description	Competency
S0023	Skill in designing security controls based on cybersecurity principles and tenets.	Computer Network Defense
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0065	Knowledge of policy-based and risk adaptive access controls.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	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
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 12. T0018 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assess the effectiveness of cybersecurity measures utilized by system(s).	Core
Entry	*Assist with documenting and assessing the effectiveness of cybersecurity measures utilized by system(s).*	
Intermediate	*Assess, validate, and document the effectiveness of cybersecurity measures utilized by system(s).*	
Advanced	*Report and consult with senior leadership on the effectiveness of cybersecurity measures utilized by system(s).*	

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

KSA ID	Description	Competency
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 14. T0019 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	Core
Entry	*Assist with the identification of threats and vulnerabilities of computer system(s) to develop a security risk profile.*	
Intermediate	*Assess, validate, and document threats to and vulnerabilities of computer system(s) to develop a security risk profile.*	
Advanced	*Brief senior leadership on threats and vulnerabilities of computer system(s) and present a security risk profile.*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0308	Knowledge of cryptology.	Encryption
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0065	Knowledge of policy-based and risk adaptive access controls.	Identity Management
K0336	Knowledge of access authentication methods.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information 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
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management

KSA ID	Description	Competency
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment

Table 16. T0021 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Build, test, and modify product prototypes using working models or theoretical models.	Core
Entry	*Assist with building, testing, and modifying product prototypes using working models or theoretical models.*	
Intermediate	*Build, test, and modify product prototypes using working models or theoretical models.*	
Advanced	*Recommend and oversee the building, testing, and modifying product prototypes using working models or theoretical models.*	

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

KSA ID	Description	Competency
K0018	Knowledge of encryption algorithms	Encryption
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0067	Knowledge of process engineering concepts.	Enterprise Architecture
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).	Identity Management
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
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
K0322	Knowledge of embedded systems.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration

Table 18. T0032 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Core
Entry	*Assist with the assessment of an application's security design for the appropriate security and privacy controls, in support of the completion of the Privacy Impact Assessments (PIAs)*	
Intermediate	*Assess an application's security design for the appropriate security and privacy controls, in support of the completion of the Privacy Impact Assessments (PIAs)*	
Advanced	*Recommend corrective actions, if needed, and report to senior leadership the application security design results of the Privacy Impact Assessments (PIA).*	

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

KSA ID	Description	Competency
K0066	Knowledge of Privacy Impact Assessments.	Data Privacy and Protection
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Data Privacy and Protection
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection
K0336	Knowledge of access authentication methods.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 20. T0053 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design and develop cybersecurity or cybersecurity-enabled products.	Core
Entry	*Assist with the design and development of cybersecurity (or cybersecurity-enabled) products.*	
Intermediate	*Design and develop cybersecurity (or cybersecurity-enabled) products.*	
Advanced	*Lead the design and development of cybersecurity (or cybersecurity-enabled) products.*	

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

KSA ID	Description	Competency
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design

Table 22. T0055 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design hardware, operating systems, and software applications to adequately address cybersecurity requirements.	Core
Entry	*Assist with the design of hardware, operating systems, and / or software applications to adequately address cybersecurity requirements.*	
Intermediate	*Design hardware, operating systems, and / or software applications to adequately address cybersecurity requirements.*	
Advanced	*Lead the design of hardware, operating systems, and / or software applications to adequately address cybersecurity requirements.*	

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

KSA ID	Description	Competency
K0081	*Knowledge of software development models (e.g., Waterfall Model, Spiral Model).*	*Software Development*
K0082	*Knowledge of software engineering.*	*Software Development*
K0035	*Knowledge of installation, integration, and optimization of system components.*	*Systems Integration*
K0086	*Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.*	*Systems Integration*
K0090	*Knowledge of system life cycle management principles, including software security and usability.*	*Systems Integration*
K0102	*Knowledge of the systems engineering process.*	*Systems Integration*
K0091	*Knowledge of systems testing and evaluation methods.*	*Systems Testing and Evaluation*

Table 24. T0056 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design or integrate appropriate data backup capabilities into overall system designs and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Core
Entry	*Assist with designing appropriate secure data backup capabilities in overall system designs.*	
Intermediate	*Document appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.*	
Advanced	*Design or integrate appropriate secure data backup capabilities into overall system designs.*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0308	Knowledge of cryptology.	Encryption
K0336	Knowledge of access authentication methods.	Identity Management
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0060	Knowledge of operating systems.	Operating Systems
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration
A0049	Ability to apply secure system design tools, methods and techniques.	System Administration
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration

KSA ID	Description	Competency
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	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
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0102	Knowledge of the systems engineering process.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation

Table 26. T0061 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop and direct system testing and validation procedures and documentation.	Core
Entry	*Assist with system testing and validation procedures and documentation.*	
Intermediate	*Develop and direct system testing and validation procedures and documentation.*	
Advanced	*Lead system testing and validation procedures and documentation.*	

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

KSA ID	Description	Competency
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation

Table 28. T0069 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop detailed security design documentation for component and interface specifications to support system design and development.	Core
Entry	*Assist with the development of detailed security design documentation, including, but not limited to component and interface specifications, to support system design and development.*	
Intermediate	*Develop detailed security design documentation including, but not limited to component and interface specifications, to support system design and development.*	
Advanced	*Lead the development of detailed security design documentation, including, but not limited to component and interface specifications, to support system design and development.*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0336	Knowledge of access authentication methods.	Identity Management
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment
K0060	Knowledge of operating systems.	Operating Systems
K0082	Knowledge of software engineering.	Software Development
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 30. T0070 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Core
Entry	*Support and assist the efforts to develop Disaster Recovery and Continuity of Operations plans for systems under development and participate in testing prior to systems entering a production environment.*	
Intermediate	*Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.*	
Advanced	*Review and recommend approval of Disaster Recovery and Continuity of Operations plans for systems under development after appropriate testing has been conducted prior to systems entering a production environment.*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0308	Knowledge of cryptology.	Encryption
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0067	Knowledge of process engineering concepts.	Enterprise Architecture
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture
K0336	Knowledge of access authentication methods.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0082	Knowledge of software engineering.	Software Development
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

KSA ID	Description	Competency
A0019	Ability to produce technical documentation.	Written Communication

Table 32. T0076 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.	Core
Entry	*Research and assist with developing mitigation strategies to address vulnerabilities and identify potential security changes to system or system components as needed.*	
Intermediate	*Develop risk mitigation strategies to address vulnerabilities and implement security changes to system or system components as needed.*	
Advanced	*Review and recommend approval of risk mitigation strategies to address vulnerabilities and validate the effectiveness of security changes to system or system components as needed.*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
S0023	Skill in designing security controls based on cybersecurity principles and tenets.	Computer Network Defense
K0336	Knowledge of access authentication methods.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0036	Knowledge of human-computer interaction principles.	Systems Integration
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

KSA ID	Description	Competency
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	Vulnerabilities Assessment
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment
A0019	Ability to produce technical documentation.	Written Communication

Table 34. T0107 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find workarounds for communication protocols that are not interoperable).	Core
Entry	Assist with the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find workarounds for communication protocols that are not interoperable).	
Intermediate	Identify and remediate technical problems encountered during testing and implementation of new systems (e.g., identify and find workarounds for communication protocols that are not interoperable).	
Advanced	Lead and recommend approval of the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find workarounds for communication protocols that are not interoperable).	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0308	Knowledge of cryptology.	Encryption
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).	Identity Management
K0336	Knowledge of access authentication methods.	Identity Management
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0015	Knowledge of computer algorithms.	Mathematical Reasoning
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
K0060	Knowledge of operating systems.	Operating Systems
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation

KSA ID	Description	Competency
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
A0026	Ability to analyze test data.	Systems Testing and Evaluation
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
A0019	Ability to produce technical documentation.	Written Communication

Table 36. T0122 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Implement security designs for new or existing system(s).	Core
Entry	*Assist in the implementation of security designs for new or existing system(s).*	
Intermediate	*Implement security designs for new or existing system(s).*	
Advanced	*Lead, review, and recommend approval of security designs for new or existing system(s).*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).	Identity Management
K0336	Knowledge of access authentication methods.	Identity Management
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
K0032	Knowledge of resiliency and redundancy.	Business Continuity

Table 38. T0124 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).	Core
Entry	*Assist with incorporating cybersecurity vulnerability solutions to incorporate into system designs (e.g., Cybersecurity Vulnerability Alerts).*	
Intermediate	*Evaluate current environment, identify, and incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).*	
Advanced	*Review, recommend approval, and / or develop new cybersecurity vulnerability solutions (e.g., Cybersecurity Vulnerability Alerts).*	

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

KSA ID	Description	Competency
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 40. T0181 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Core
Entry	*Assist in performing information systems security risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.*	
Intermediate	*Perform information systems security risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.*	
Advanced	*Review results and suggest corrective actions, if necessary, to mitigate identified systems security vulnerabilities (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0308	Knowledge of cryptology.	Encryption
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).	Identity Management
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0084	Knowledge of structured analysis principles and methods.	Risk Management
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment

KSA ID	Description	Competency
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
A0019	Ability to produce technical documentation.	Written Communication

Table 42. T0205 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Core
Entry	*Propose and assist with inputs to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).*	
Intermediate	*Evaluate and provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).*	
Advanced	*Lead, review, and recommend approval of activities regarding information systems security in support of the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment

KSA ID	Description	Competency
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0082	Knowledge of software engineering.	Software Development
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	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
K0090	Knowledge of system life cycle management principles, including software security and usability.	Systems Integration
K0102	Knowledge of the systems engineering process.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 44. T0228 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Core
Entry	*Assist with storing, retrieving, and manipulating data for analysis of system capabilities and requirements.*	
Intermediate	*Store, retrieve, and manipulate data for analysis of system capabilities and requirements.*	
Advanced	*Lead the storing, retrieval, and manipulation of data for analysis of system capabilities and requirements.*	

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

KSA ID	Description	Competency
K0024	Knowledge of database systems.	Database Management Systems
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0067	Knowledge of process engineering concepts.	Enterprise Architecture
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
K0015	Knowledge of computer algorithms.	Mathematical Reasoning
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
K0102	Knowledge of the systems engineering process.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation

Table 46. T0231 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provide support to security/certification test and evaluation activities.	Core
Entry	*Support systems security/certification test and evaluation activities.*	
Intermediate	*Independently conduct and support multiple systems security/certification test and evaluation activities.*	
Advanced	*Lead others in conducting systems security/certification test and evaluation activities.*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0308	Knowledge of cryptology.	Encryption
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).	Identity Management
K0336	Knowledge of access authentication methods.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design

KSA ID	Description	Competency
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
A0026	Ability to analyze test data.	Systems Testing and Evaluation

Table 48. T0269 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design and develop key management functions (as related to cybersecurity).	Core
Entry	*Observe and assist with the design and development on key management functions as it relates to cryptographic key usage.*	
Intermediate	*Design and develop key management functions (as it relates to cryptographic key usage).*	
Advanced	*Lead the implementation of key management functions (as it relates to cryptographic key usage).*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0018	Knowledge of encryption algorithms	Encryption
K0308	Knowledge of cryptology.	Encryption
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0082	Knowledge of software engineering.	Software Development
K0102	Knowledge of the systems engineering process.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation

Table 50. T0270 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Analyze user needs and requirements to plan and conduct system security development.	Core
Entry	*Gather and assist with analyzing user needs and requirements to plan and conduct system security development.*	
Intermediate	*Analyze and document user needs and requirements to plan and conduct system security development.*	
Advanced	*Recommend enhancements based on user needs and requirements to plan and conduct system security development.*	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
S0023	Skill in designing security controls based on cybersecurity principles and tenets.	Computer Network Defense
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture
A0061	Ability to design architectures and frameworks.	Enterprise Architecture
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).	Identity Management
K0065	Knowledge of policy-based and risk adaptive access controls.	Identity Management
K0336	Knowledge of access authentication methods.	Identity Management
S0031	Skill in developing and applying security system access controls.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—to leverage analytical and technical expertise.	Interpersonal Skills
A0098	Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.	Interpersonal Skills
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	Organizational Awareness

KSA ID	Description	Competency
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development
K0082	Knowledge of software engineering.	Software Development
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration
A0049	Ability to apply secure system design tools, methods and techniques.	System Administration
A0050	Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools.	System Administration
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0102	Knowledge of the systems engineering process.	Systems Integration

Table 52. T0272 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	Core
Entry	*Assist with identifying and documenting security design and cybersecurity development activities. (providing a functional description of security implementation) and update as necessary.*	
Intermediate	*Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.*	
Advanced	*Develop business processes to ensure that security design and cybersecurity development activities are properly documented and updated as necessary.*	

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

KSA ID	Description	Competency
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
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
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
A0074	Ability to collaborate effectively with others.	Interpersonal Skills
A0098	Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.	Interpersonal Skills
A0012	Ability to ask clarifying questions.	Oral Communication
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development
K0082	Knowledge of software engineering.	Software Development
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	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
K0102	Knowledge of the systems engineering process.	Systems Integration

KSA ID	Description	Competency
A0019	Ability to produce technical documentation.	Written Communication

Table 54. T0304 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	Core
Entry	Participate in the system development life cycle (SDLC) methodologies processes (e.g., IBM Rational Unified Process) with regards the development environment.	
Intermediate	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	
Advanced	Lead and validate the integration of system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process).	

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

KSA ID	Description	Competency
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security

Table 56. T0326 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Employ configuration management processes.	Core
Entry	Assist with employing configuration management processes.	
Intermediate	Employ configuration management processes.	
Advanced	Lead the employment of configuration management processes.	

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

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0067	Knowledge of process engineering concepts.	Enterprise Architecture
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment
K0082	Knowledge of software engineering.	Software Development
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration

Table 58. T0359 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	Core
Entry	Assist with testing and evaluating secure interfaces between information systems, physical systems, and/or embedded technologies.	
Intermediate	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	
Advanced	Lead the design, implementation, testing, and evaluation of secure interfaces between information systems, physical systems, and/or embedded technologies.	

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

KSA ID	Description	Competency
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design
K0322	Knowledge of embedded systems.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation

Table 60. T0446 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.	Core
Entry	Assist with developing, integrating, and updating system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.	
Intermediate	Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.	
Advanced	Lead, review, and recommend approval of the design, development, integration and update of system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.	

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

KSA ID	Description	Competency
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0102	Knowledge of the systems engineering process.	Systems Integration

Table 62. T0449 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design to security requirements to ensure requirements are met for all systems and/or applications.	Core
Entry	*Assist with designing to security controls to ensure requirements are met for all systems and/or applications.*	
Intermediate	*Design security controls to ensure requirements are met for all systems and/or applications.*	
Advanced	*Lead, evaluate, and recommend approval on designs that meet the necessary security controls to ensure requirements are met for all systems and/or applications.*	

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

KSA ID	Description	Competency
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	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
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 64. T0509 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform an information security risk assessment.	Core
Entry	*Assist with performing an information security risk assessment.*	
Intermediate	*Perform and document the results of an information security risk assessment.*	
Advanced	*Provide the results of an information security risk assessment to senior leadership and recommend corrective action, if necessary, to mitigate identified information's systems security.*	

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

KSA ID	Description	Competency
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 66. T0518 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform security reviews and identify security gaps in architecture.	Core
Entry	*Assist with performing security reviews and identify security gaps in architecture.*	
Intermediate	*Perform security reviews and identify security gaps in architecture and provide recommendations based on the gaps.*	
Advanced	*Review and recommend approval of corrective actions that address security gaps in architecture to senior leadership.*	

Table 67. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0032	Knowledge of resiliency and redundancy.	Business Continuity
K0308	Knowledge of cryptology.	Encryption
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0067	Knowledge of process engineering concepts.	Enterprise Architecture
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture
A0008	Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).	Enterprise Architecture
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).	Identity Management
K0065	Knowledge of policy-based and risk adaptive access controls.	Identity Management
K0336	Knowledge of access authentication methods.	Identity Management
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
K0045	Knowledge of information security systems engineering principles (NIST SP 800-160).	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security

KSA ID	Description	Competency
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
S0085	Skill in conducting audits or reviews of technical systems.	Information Technology Assessment
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
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
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design
K0322	Knowledge of embedded systems.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
A0040	Ability to translate data and test results into evaluative conclusions.	Problem Solving
K0084	Knowledge of structured analysis principles and methods.	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
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
A0026	Ability to analyze test data.	Systems Testing and Evaluation
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
K0297	Knowledge of countermeasure design for identified security risks.	Threat Analysis
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment