5

CAREER PATHWAY SECURE SOFTWARE ASSESSOR (622)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 622-SECURE SOFTWARE ASSESSOR

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 622-Secure Software Assessor.

Table 1. 622-Secure Software Assessor Work Role Overview

NICE Role Description	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.
OPM Occupational Series	Personnel performing the 622-Secure Control Assessor work role are most commonly aligned to the following Occupational Series: - 2210-Information Technology – 65% - 1550-Computer Science – 15% - 0854-Computer Engineering – 7% - 0855-Electronics Engineering – 5% - 2003-Supply Program Management – 3% - 0801-General Engineering – 3%
Work Role Pairings	Personnel performing the 622-Secure Control Assessor work role are most commonly paired with the following complimentary Work Roles (Top 6 shown): - 621-Software Developer – 44% - 641-Systems Requirements Planner – 17% - 671-System Testing and Evaluation Specialist – 11% - 451-System Administrator – 4% - 411-Technical Support Specialist – 3% - 461-Systems Security Analyst – 3%
Functional Titles	Personnel performing the 622-Secure Control Assessor work role may unofficially or alternatively be called (Top 5 shown): - Information Assurance (IA) Software Developer - Information Assurance (IA) Software Engineer - Security Engineer - Secure Software Engineer - Application Security Analyst/Engineer - Application Security Tester - Software Quality / Quality Assurance Engineer - Software Assurance Analyst - Security Requirements Analyst

Distribution of GS-Levels	Personnel performing the 622-Secure Software Assessor work role are most commonly found within the following grades on the General Schedule*: - ☐ GS-7 – redacted** - ☐ GS-9 – redacted** - ☒ GS-11 – 10% - ☒ GS-12 – 27% - ☒ GS-13 – 22% - ☒ GS-14 – 6% - ☒ GS-15 – 4% *32% of all 622s 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 622-Secure Software Assessor work role: - 621-Software Developer - 661-Research & Development Specialist - 671-System Testing and Evaluation Specialist
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 622-Secure Software Assessor. This is not an exhaustive list, nor does it consider learning and development opportunities an individual may pursue to prepare themselves for performing alternate work roles: - 661-Research and Development Specialist - 671-System Testing and Evaluation Specialist - 541-Vulnerability Assessment Analyst - 612-Security Control Assessor - 722-Information Systems Security Manager *Note: Leveraging the knowledge, skills, abilities, and tasks of the 622-Secure Software Assessor 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* - *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 622-Secure Software Assessor work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 622-Secure Software Assessor Core Tasks

Task ID	Task	Core or Additional
T0456	Develop secure software testing and validation procedures.	Core
T0516	Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.	Core
T0217	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Core
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Core
T0013	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	Core
T0554	Determine and document software patches or the extent of releases that would leave software vulnerable.	Core
T0118	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	Core
T0111	Identify basic common coding flaws at a high level.	Core
T0040	Consult with engineering staff to evaluate interface between hardware and software.	Core
T0022	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	Additional
T0236	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	Additional
T0457	Develop system testing and validation procedures, programming, and documentation.	Additional
T0436	Conduct trial runs of programs and software applications to ensure the desired information is produced and instructions and security levels are correct.	Additional
T0171	Perform integrated quality assurance testing for security functionality and resiliency attack.	Additional
T0311	Consult with customers about software system design and maintenance.	Additional
T0117	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development.	Additional
T0424	Analyze and provide information to stakeholders that will support the development of security an application or modification of an existing security application.	Additional

Task ID	Task	Core or Additional
T0428	Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.	Additional
T0038	Develop threat model based on customer interviews and requirements.	Additional
T0266	Perform penetration testing as required for new or updated applications.	Additional
T0324	Direct software programming and development of documentation.	Additional
T0228	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Additional
T0337	Supervise and assign work to programmers, designers, technologists and technicians and other engineering and scientific personnel.	Additional
T0014	Apply secure code documentation.	Additional
T0100	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	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 622-Secure Software Assessor work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 622-Secure Software Assessor Core Knowledge, Skills, and Abilities

KSA ID	KSA 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
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Core
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Core
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security	Core
K0060	Knowledge of operating systems.	Operating Systems	Core
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management	Core
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development	Core
K0153	Knowledge of software quality assurance process.	Software Development	Core
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	Software Development	Core
S0174	Skill in using code analysis tools.	Software Testing and Evaluation	Core
K0073	Knowledge of secure configuration management techniques.	System Administration	Core
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation	Core
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	Systems Testing and Evaluation	Core
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis	Core
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race	Vulnerabilities Assessment	Core

KSA ID	KSA Description	Competency	Importance to Work Role
	conditions, covert channel, replay, return-oriented attacks, malicious code).		
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment	Core
K0014	Knowledge of complex data structures.	Computer Languages	Additional
K0016	Knowledge of computer programming principles such as object-oriented design.	Computer Languages	Additional
K0051	Knowledge of low-level computer languages (e.g., assembly languages).	Computer Languages	Additional
K0068	Knowledge of programming language structures and logic.	Computer Languages	Additional
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages	Additional
K0140	Knowledge of secure coding techniques.	Computer Languages	Additional
K0202	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).	Computer Network Defense	Additional
A0021	Ability to use and understand complex mathematical concepts (e.g., discrete math).	Data Analysis	Additional
K0066	Knowledge of Privacy Impact Assessments.	Data Privacy and Protection	Additional
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Data Privacy and Protection	Additional
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection	Additional
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption	Additional
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zackman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture	Additional
S0031	Skill in developing and applying security system access controls.	Identity Management	Additional
K0343	Knowledge of root cause analysis techniques.	Incident Management	Additional
S0175	Skill in performing root cause analysis.	Incident Management	Additional
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance	Additional
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	Information Systems/Network Security	Additional
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Additional

KSA ID	KSA Description	Competency	Importance to Work Role
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment	Additional
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design	Additional
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Infrastructure Design	Additional
K0322	Knowledge of embedded systems.	Infrastructure Design	Additional
K0084	Knowledge of structured analysis principles and methods.	Risk Management	Additional
K0154	Knowledge of supply chain risk management standards, processes, and practices.	Risk Management	Additional
K0079	Knowledge of software debugging principles.	Software Development	Additional
K0080	Knowledge of software design tools, methods, and techniques.	Software Development	Additional
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development	Additional
K0082	Knowledge of software engineering.	Software Development	Additional
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration	Additional
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment	Additional
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.	Vulnerabilities Assessment	Additional
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	Web Technology	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 622-Secure Software Assessor 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. 622-Secure Software Assessor Core Competencies

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Computer Languages	C006	Computer languages and their applications to enable a system to perform specific functions.	• Knowledge of complex data structures. [K0014] • Knowledge of computer programming principles such as object-oriented design. [K0016] • Knowledge of low-level computer languages (e.g., assembly languages). [K0051] • Knowledge of programming language structures and logic. [K0068] • Knowledge of interpreted and compiled computer languages. [K0139] • Knowledge of secure coding techniques. [K0140]	Core
Data Privacy and Protection	C014	Relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them	• Knowledge of Personally Identifiable Information (PII) data security standards. [K0260] • Knowledge of Privacy Impact Assessments. [K0066] • Knowledge of Payment Card Industry (PCI) data security standards. [K0261] • Knowledge of Personal Health Information (PHI) data security standards. [K0262]	Core
Information Assurance	C022	Methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	• Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [K0044] • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [A0123] • Knowledge of organization's enterprise information security architecture system. [K0027] • Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [S0367]Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [S0367]	Core
Software Development	C045	Collective processes involved in creating software programs, embodying all the stages throughout the	• Knowledge of cybersecurity principles and methods that apply to software development. [K0039] • Knowledge of software quality assurance process. [K0153] • Knowledge of secure software deployment methodologies, tools, and practices. [K0178] • Knowledge of software debugging principles. [K0079]	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
		systems development life cycle	• Knowledge of software design tools, methods, and techniques. [K0080] • Knowledge of software development models (e.g., Waterfall Model, Spiral Model). [K0081] • Knowledge of software engineering. [K0082]	
Systems Testing and Evaluation	C050	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 organization's evaluation and validation requirements. [K0028] • Skill in secure test plan design (e. g. unit, integration, system, acceptance). [S0135]	Core
Vulnerabilities Assessment	C057	Principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	• Knowledge of cyber threats and vulnerabilities. [K0005] • Knowledge of specific operational impacts of cybersecurity lapses. [K0006] • Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). [K0070] • Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. [S0001] • Knowledge of penetration testing principles, tools, and techniques. [K0342] • Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) [K0624] • Skill in integrating black box security testing tools into quality assurance process of software releases. [S0083] • Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language. [K0105]	Core
Risk Management	C044	Methods and tools used for risk assessment and mitigation of risk.	• Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). [K0002] • Knowledge of information technology (IT) risk management policies, requirements, and procedures. [K0263] • Knowledge of structured analysis principles and methods. [K0084] • Knowledge of supply chain risk management standards, processes, and practices. [K0154]	Additional
Infrastructure Design	C026	Architecture and typology of software, hardware, and networks, including LANS, WANS, and	• Knowledge of computer networking concepts and protocols, and network security methodologies. [K0001] • Knowledge of local area and wide area networking principles and concepts including bandwidth management. [K0050]	Additional

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
		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 local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability. [K0170] • Knowledge of embedded systems. [K0322]	
Information Systems/ Network Security	C024	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. [K0004] • Skill in discerning the protection needs (i.e., security controls) of information systems and networks. [S0034] • Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization). [K0152] • Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). [K0179]	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 622-Secure Software Assessor Suggested Qualifications / Capability Indicators

For indicators of capability for the 622-Secure Software Assessor 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 622-Secure Software Assessor.

2 APPENDIX: 622-SECURE SOFTWARE ASSESSOR 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.

2.2 622-Secure Software Assessor Task Analysis and KSA Mapping

Table 8. T0456 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop secure software testing and validation procedures.	Core
Entry	*Implement secure software testing and validation procedures.*	
Intermediate	*Develop [and modify] secure software testing and validation procedures [in accordance with Federal and Department security and privacy policies and guidelines].*	
Advanced	*Assess and approve secure software testing and validation procedures.*	

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

KSA ID	Description	Competency
K0016	Knowledge of computer programming principles such as object-oriented design.	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages
K0140	Knowledge of secure coding techniques.	Computer Languages
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0066	Knowledge of Privacy Impact Assessments.	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
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zackman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture
K0343	Knowledge of root cause analysis techniques.	Incident Management
S0175	Skill in performing root cause analysis.	Incident Management
K0044	Knowledge of cybersecurity principles and 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
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to 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
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	Information Systems/Network Security

KSA ID	Description	Competency
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Infrastructure Design
K0322	Knowledge of embedded systems.	Infrastructure Design
K0060	Knowledge of operating systems.	Operating Systems
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0154	Knowledge of supply chain risk management standards, processes, and practices.	Risk Management
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development
K0153	Knowledge of software quality assurance process.	Software Development
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	Software Development
K0079	Knowledge of software debugging principles.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
K0073	Knowledge of secure configuration management techniques.	System Administration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	Systems Testing and Evaluation
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.	Vulnerabilities Assessment
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	Web Technology

Table 10. T0516 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.	Core
Entry	*Perform routine secure program testing, review, and/or assessment and initial analysis of results to identify potential flaws in codes and mitigate vulnerabilities.*	
Intermediate	*Review results and validate identified flaws as vulnerabilities in light of agency-specific context to the results, which may alter the outcome of the assessment.*	
Advanced	*Validate identified flaws as vulnerabilities and recommend corrective action.*	

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

KSA ID	Description	Competency
K0016	Knowledge of computer programming principles such as object-oriented design.	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0140	Knowledge of secure coding techniques.	Computer Languages
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0066	Knowledge of Privacy Impact Assessments.	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
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zackman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture
S0031	Skill in developing and applying security system access controls.	Identity Management
K0343	Knowledge of root cause analysis techniques.	Incident Management
S0175	Skill in performing root cause analysis.	Incident Management
K0044	Knowledge of cybersecurity principles and 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
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security

KSA ID	Description	Competency
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	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
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment
K0322	Knowledge of embedded systems.	Infrastructure Design
K0060	Knowledge of operating systems.	Operating Systems
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0154	Knowledge of supply chain risk management standards, processes, and practices.	Risk Management
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development
K0153	Knowledge of software quality assurance process.	Software Development
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	Software Development
K0079	Knowledge of software debugging principles.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development
K0082	Knowledge of software engineering.	Software Development
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
K0073	Knowledge of secure configuration management techniques.	System Administration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment

KSA ID	Description	Competency
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.	Vulnerabilities Assessment
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	Web Technology

Table 12. T0217 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Core
Entry	*Identify and/or report security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.*	
Intermediate	*[Review and validate identified] security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.*	
Advanced	*Recommend corrective actions for addressing security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.*	

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

KSA ID	Description	Competency
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
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
K0343	Knowledge of root cause analysis techniques.	Incident Management
S0175	Skill in performing root cause analysis.	Incident Management
K0044	Knowledge of cybersecurity principles and 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
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to 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
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	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
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Infrastructure Design
K0060	Knowledge of operating systems.	Operating Systems
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development

KSA ID	Description	Competency
K0153	Knowledge of software quality assurance process.	Software Development
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	Software Development
K0079	Knowledge of software debugging principles.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
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.	System Administration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.	Vulnerabilities Assessment
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	Web Technology

Table 14. 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	*Perform the risk analysis and identify potential threats, vulnerabilities, and probability of occurrence whenever an application or system undergoes a major change.*	
Intermediate	*[Validate initial analysis of] threats, vulnerability and probability of occurrence whenever an application or system undergoes a major change.*	
Advanced	*Recommend corrective action to address threats, vulnerabilities, and probability of occurrence whenever an application or system undergoes a major change.*	

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

KSA ID	Description	Competency
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages
K0140	Knowledge of secure coding techniques.	Computer Languages
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
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption
K0343	Knowledge of root cause analysis techniques.	Incident Management
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	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
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Infrastructure Design
K0322	Knowledge of embedded systems.	Infrastructure Design
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0154	Knowledge of supply chain risk management standards, processes, and practices.	Risk Management
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	Software Development

KSA ID	Description	Competency
K0073	Knowledge of secure configuration management techniques.	System Administration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	Web Technology

Table 16. T0013 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	Core
Entry	*Apply security testing tools and techniques using accepted coding and testing standards and assist with conducting code reviews.*	
Intermediate	*Apply security testing tools [and techniques using accepted coding and testing standards and conduct code reviews.]*	
Advanced	*Apply advanced security testing tools and techniques using accepted coding and testing standards and conduct code reviews.*	

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

KSA ID	Description	Competency
K0016	Knowledge of computer programming principles such as object-oriented design.	Computer Languages
K0051	Knowledge of low-level computer languages (e.g., assembly languages).	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages
K0140	Knowledge of secure coding techniques.	Computer Languages
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
K0044	Knowledge of cybersecurity principles and 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
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	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
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Infrastructure Design
K0060	Knowledge of operating systems.	Operating Systems
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0154	Knowledge of supply chain risk management standards, processes, and practices.	Risk Management
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development
K0153	Knowledge of software quality assurance process.	Software Development
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	Software Development
K0079	Knowledge of software debugging principles.	Software Development

KSA ID	Description	Competency
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development
K0082	Knowledge of software engineering.	Software Development
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
K0073	Knowledge of secure configuration management techniques.	System Administration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	Systems Testing and Evaluation
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.	Vulnerabilities Assessment
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	Web Technology

Table 18. T0554 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Determine and document software patches or the extent of releases that would leave software vulnerable.	Core
Entry	*Determine and document software patches or the extent of releases that would leave software vulnerable.*	
Intermediate	*Validate the extent that the software patch leaves the software vulnerable.*	
Advanced	*Recommend corrective action to reduce the extent of software vulnerability.*	

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

KSA ID	Description	Competency
K0140	Knowledge of secure coding techniques.	Computer Languages
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
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption
K0343	Knowledge of root cause analysis techniques.	Incident Management
K0044	Knowledge of cybersecurity principles and 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
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	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
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Infrastructure Design
K0322	Knowledge of embedded systems.	Infrastructure Design
K0060	Knowledge of operating systems.	Operating Systems
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0154	Knowledge of supply chain risk management standards, processes, and practices.	Risk Management
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development
K0153	Knowledge of software quality assurance process.	Software Development
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	Software Development

KSA ID	Description	Competency
K0079	Knowledge of software debugging principles.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
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.	System Administration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	Systems Testing and Evaluation
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.	Vulnerabilities Assessment
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	Web Technology

Table 20. T0118 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	Core
Entry	*Assist with identifying security issues around steady state operation and management of software.*	
Intermediate	*Identify and validate security issues around steady state operation and management of software.*	
Advanced	*Recommend security measures that must be taken while maintaining or replacing a product when it reaches its end of life.*	

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

KSA ID	Description	Competency
K0140	Knowledge of secure coding techniques.	Computer Languages
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0066	Knowledge of Privacy Impact Assessments.	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
K0044	Knowledge of cybersecurity 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
K0322	Knowledge of embedded systems.	Infrastructure Design
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development
K0073	Knowledge of secure configuration management techniques.	System Administration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment

Table 22. T0111 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify basic common coding flaws at a high level.	Core
Entry	*Identify basic coding flaws at a high level.*	
Intermediate	*Identify coding flaws.*	
Advanced	*Identify complex coding flaws and recommend mitigating solutions.*	

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

KSA ID	Description	Competency
K0016	Knowledge of computer programming principles such as object-oriented design.	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages
K0140	Knowledge of secure coding techniques.	Computer Languages
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
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption
K0044	Knowledge of cybersecurity principles and 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
K0027	Knowledge of organization's enterprise information security architecture system.	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	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
K0322	Knowledge of embedded systems.	Infrastructure Design
K0060	Knowledge of operating systems.	Operating Systems
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development
K0153	Knowledge of software quality assurance process.	Software Development
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	Software Development
K0079	Knowledge of software debugging principles.	Software Development

KSA ID	Description	Competency
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
K0073	Knowledge of secure configuration management techniques.	System Administration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	Web Technology

Table 24. T0040 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Consult with engineering staff to evaluate interface between hardware and software.	Core
Entry	*Consult with engineering staff to evaluate secure implementations between hardware and software.*	
Intermediate	*Consult with engineering staff to recommend corrective action to mitigate identified risks between hardware and software.*	
Advanced	*Consult with engineering staff to recommend corrective action to mitigate identified risks between hardware and software.*	

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

KSA ID	Description	Competency
K0044	Knowledge of cybersecurity 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
K0060	Knowledge of operating systems.	Operating Systems
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	Software Development
K0153	Knowledge of software quality assurance process.	Software Development
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	Software Development
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
K0073	Knowledge of secure configuration management techniques.	System Administration
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zackman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture
S0175	Skill in performing root cause analysis.	Incident Management
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	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
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	Infrastructure Design

KSA ID	Description	Competency
K0322	Knowledge of embedded systems.	Infrastructure Design
K0079	Knowledge of software debugging principles.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.	Vulnerabilities Assessment
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	Web Technology