CAREER PATHWAY SOFTWARE DEVELOPER (621)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 621-SOFTWARE DEVELOPER

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 621-Software Developer.

Table 1. 621-Software Developer Work Role Overview

NICE Role Description	*Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.*
OPM Occupational Series	Personnel performing the 621-Software Developer work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 60% - 1550-Computer Science – 26% - 0854-Computer Engineering – 7% - 0855-Electronics Engineering – 4% - 0850-Electrical Engineering – 1%
Work Role Pairings	Personnel performing the 651-Enterprise Architect work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 632-Systems Developer – 44% - 641-Systems Requirements Planner – 11% - 671-System Testing and Evaluation Specialist – 7% - 422-Data Analyst – 7% - 411-Technical Support Specialist – 4%
Functional Titles	Personnel performing the 621-Software Developer work role may unofficially or alternatively be called: - Analyst Programmer - Computer Programmer - Configuration Manager - Information Assurance (IA) Software Developer/Engineer - Secure Software Engineer - Software Engineer/Architect - Web Application Developer - Cloud Developer - Mainframe Developer - Full Stack Developer
Distribution of GS-Levels	Personnel performing the 621-Software Developer are most commonly found within the following grades on the General Schedule. * - ☐ GS-3 – redacted**

	- ☐ GS-4 – redacted** - ☐ GS-5 – redacted** - ☐ GS-7– redacted** - ☐ GS-9 – redacted** - ☐ GS-10 – redacted** - ☒ GS-11 – 6% - ☒ GS-12 – 24% - ☒ GS-13 – 25% - ☒ GS-14 – 8% - ☐ GS-15 – redacted** *34% of all 621s 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 621-Software Developer work role: - 421-Database Administrator - 422-Data Analyst - 451-System Administrator - 641-Systems Requirements Planner - 411-Technical Support Specialist - 461-Systems Security Analyst
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 621-Software Developer. 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: - 422-Data Analyst - 632-Systems Developer - 641-Systems Requirements Planner - 651-Enterprise Architect - 661-Research and Development Specialist - 212-Cyber Defense Forensics Analyst - 461-Systems Security Analyst - 622-Secure Software Assessor *Note: Leveraging the knowledge, skills, abilities, and tasks of the 621-Software 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* - *803-Product Support Manager*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 621-Software Developer work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 621-Software Developer Core Tasks

Task ID	Task Description	Core or Additional
T0009	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.	Core
T0011	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.	Core
T0013	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	Core
T0553	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Core
T0014	Apply secure code documentation.	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.	Core
T0026	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.	Core
T0436	Conduct trial runs of programs and software applications to ensure the desired information is produced and instructions and security levels are correct.	Core
T0034	Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.	Core
T0040	Consult with engineering staff to evaluate interface between hardware and software.	Core
T0046	Correct errors by making appropriate changes and rechecking the program to ensure desired results are produced.	Core
T0057	Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.	Core
T0554	Determine and document software patches or the extent of releases that would leave software vulnerable.	Core
T0077	Develop secure code and error handling.	Core
T0455	Develop software system testing and validation procedures, programming, and documentation.	Core
T0416	Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.	Core
T0100	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Core
T0417	Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise AV solution) when appropriate.	Core

Task ID	Task Description	Core or Additional
T0111	Identify basic common coding flaws at a high level.	Core
T0117	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development.	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
T0500	Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.	Core
T0171	Perform integrated quality assurance testing for security functionality and resiliency attack.	Core
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Core
T0176	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.	Core
T0228	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Core
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.	Core
T0217	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Additional
T0311	Consult with customers about software system design and maintenance.	Additional
T0267	Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.	Additional
T0324	Direct software programming and development of documentation.	Additional
T0303	Identify and leverage the enterprise-wide version control system while designing and developing secure applications.	Additional
T0189	Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language.	Additional
T0337	Supervise and assign work to programmers, designers, technologists and technicians and other engineering and scientific personnel.	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 621-Software Developer work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 621-Software Developer Core KSAs

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
K0016	Knowledge of computer programming principles	Computer Languages	Core
K0051	Knowledge of low-level computer languages (e.g., assembly languages).	Computer Languages	Core
K0068	Knowledge of programming language structures and logic.	Computer Languages	Core
K0139	Knowledge of interpreted and compiled computer languages.	Computer Languages	Core
K0140	Knowledge of secure coding techniques.	Computer Languages	Core
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Core
S0031	Skill in developing and applying security system access controls.	Identity Management	Core
K0343	Knowledge of root cause analysis techniques.	Incident Management	Core
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Core

KSA ID	Description	Competency	Importance to Work Role
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	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
K0084	Knowledge of structured analysis principles and methods.	Risk Management	Core
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management	Core
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	Software Development	Core
K0079	Knowledge of software debugging principles.	Software Development	Core
K0080	Knowledge of software design tools, methods, and techniques.	Software Development	Core
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	Software Development	Core
K0082	Knowledge of software engineering.	Software Development	Core
K0153	Knowledge of software quality assurance process.	Software Development	Core
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development	Core
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development	Core
S0014	Skill in conducting software debugging.	Software Testing and Evaluation	Core
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration	Core
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration	Core

KSA ID	Description	Competency	Importance to Work Role
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation	Core
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	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 conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment	Core
K0105	Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web service description language).	Web Technology	Core
K0014	Knowledge of complex data structures.	Computer Languages	Additional
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	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
S0017	Skill in creating and utilizing mathematical or statistical models.	Data Analysis	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

KSA ID	Description	Competency	Importance to Work Role
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., Zachman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture	Additional
S0175	Skill in performing root cause analysis.	Incident Management	Additional
K0027	Knowledge of organization's enterprise information security architecture.	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
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	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
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	Infrastructure Design	Additional
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design	Additional
K0322	Knowledge of embedded systems.	Infrastructure Design	Additional
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design	Additional
K0060	Knowledge of operating systems.	Operating Systems	Additional

KSA ID	Description	Competency	Importance to Work Role
K0154	Knowledge of supply chain risk management standards, processes, and practices.	Risk Management	Additional
S0174	Skill in using code analysis tools.	Software Testing and Evaluation	Additional
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation	Additional
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	Systems Testing and Evaluation	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
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 621-Software 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. 621-Software Developer Core Competencies

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Computer Languages	C006	This area contains KSAs that relate to computer languages and their applications to enable a system to perform specific functions.	• Knowledge of complex data structures. (K0014) • Knowledge of secure coding techniques. (K0140) • Knowledge of programming language structures and logic. (K0068) • Knowledge of computer programming principles. (K0016) • Skill in writing code in a currently supported programming language (e.g., Java, C++). (S0060) • Knowledge of interpreted and compiled computer languages. (K0139) • Knowledge of low-level computer languages (e.g., assembly languages). (K0051)	Core
Information Systems/ Network Security	C024	This area contains 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.	• 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 cybersecurity and privacy principles. (K0004) • Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). (K0179)	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Software Development	C045	This area contains KSAs that relate to the collective processes involved in creating software programs, embodying all the stages throughout the systems development life cycle	• Skill in developing applications that can log and handle errors, exceptions, and application faults and logging. (S0149) • Knowledge of software engineering. (K0082) • Knowledge of software development models (e.g., Waterfall Model, Spiral Model). (K0081) • Knowledge of software quality assurance process. (K0153) • Knowledge of software debugging principles. (K0079) • Ability to develop secure software according to secure software deployment methodologies, tools, and practices. (A0047) • Knowledge of software design tools, methods, and techniques. (K0080)	Core
Software Testing and Evaluation	C046	This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering software test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.	• Ability to tailor code analysis for application-specific concerns. (A0007) • Skill in using code analysis tools. (S0174) • Skill in conducting software debugging. (S0014)	Core
Risk Management	C044	This area contains KSAs that relate to the methods and tools used for risk assessment and mitigation of risk.	• Knowledge of supply chain risk management standards, processes, and practices. (K0154) • Knowledge of structured analysis principles and methods. (K0084) • Knowledge of information technology (IT) risk management policies, requirements, and procedures. (K0263) • Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). (K0002)	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Vulnerabilities Assessment	C057	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	• Knowledge of specific operational impacts of cybersecurity lapses. (K0006) • Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. (S0001) • 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) • Knowledge of cyber threats and vulnerabilities. (K0005) • Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list). (K0624) • Knowledge of penetration testing principles, tools, and techniques. (K0342)	Core
Data Privacy and Protection	C014	This area contains 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. (K0066) • Knowledge of Personally Identifiable Information (PII) data security standards. (K0260) • Knowledge of Payment Card Industry (PCI) data security standards. (K0261) • Knowledge of Personal Health Information (PHI) data security standards. (K0262)	Additional
Information Assurance	C022	This area contains KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	• Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (S0367) • Knowledge of organization's enterprise information security architecture. (K0027) • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (A0123) • Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (K0044)	Additional

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Infrastructure Design	C026	This area contains 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 local area and wide area networking principles and concepts including bandwidth management. (K0050) • Knowledge of computer networking concepts and protocols, and network security methodologies. (K0001) • Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. (K0332) • Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. (K0170) • Knowledge of embedded systems. (K0322)	Additional
Systems Testing and Evaluation	C050	This area contains 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 organization's evaluation and validation requirements. (K0028) • Skill in secure test plan design (e. g. unit, integration, system, acceptance). (S0135) • Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams. (S0019)	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 621-Software Developer Suggested Qualifications

For indicators of capability for 621-Software 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 621-Software Developer.

2 APPENDIX: 621-SOFTWARE 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.

2.2 621-SOFTWARE DEVELOPER TASK ANALYSIS AND KSA MAPPING

Table 8. T0009 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.	Core
Entry	*Assist in analyzing information that will be used to determine, recommend, and plan the development of a new application or modification of an existing application. Assist in trade-off analysis.*	
Intermediate	*Analyze information that will be used to determine, recommend, and plan the development of a new application or modification of an existing application. Conduct in trade-off analysis. Conduct peer review.*	
Advanced	*Teach/conduct analysis of information and determine, recommend, and plan the development of a new application or modification of an existing application. Identify gaps in capabilities and automation opportunities.*	

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

KSA ID	Description	Competency
K0014	Knowledge of complex data structures.	Computer Languages
K0016	Knowledge of computer programming principles	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
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
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
K0343	Knowledge of root cause analysis techniques.	Incident Management
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
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
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

KSA ID	Description	Competency
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	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
K0153	Knowledge of software quality assurance process.	Software Development
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
S0014	Skill in conducting software debugging.	Software Testing and Evaluation
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	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
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
K0105	Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web service description language).	Web Technology

Table 10. T0011 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.	Core
Entry	*Apply, under supervision, secure code documentation guidelines provided.*	
Intermediate	*Determine what guidelines are applicable with minimal oversight. Apply and contribute to secure code documentation guidelines.*	
Advanced	*Develop secure coding techniques documentation. Provide guidance/supervision to others.*	

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

KSA ID	Description	Competency
K0014	Knowledge of complex data structures.	Computer Languages
K0016	Knowledge of computer programming principles	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
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
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
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
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation

Table 12. 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	*Demonstrates knowledge of coding and testing standards, how to apply security testing tools including "fuzzy" static-analysis code scanning tools, and conducting code reviews.*	
Intermediate	*Develop coding and testing standards and security testing tools including "fuzzy" static-analysis code scanning tools, and oversee code reviews.*	
Advanced	*Review and approve coding and testing standards, security testing tools including "fuzzy" static-analysis code scanning tools, and code reviews.*	

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

KSA ID	Description	Competency
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	Systems Testing and Evaluation
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	Systems Testing and Evaluation
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
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment

Table 14. T0553 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Core
Entry	*Assist with the application of cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.*	
Intermediate	*Apply complex or novel cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.*	
Advanced	*Oversee the application of cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.*	

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

KSA ID	Description	Competency
S0031	Skill in developing and applying security system access controls.	Identity Management
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	Software Development
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment

Table 16. T0014 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Apply secure code documentation.	Core
Entry	*Apply, under supervision, secure code documentation guidelines provided.*	
Intermediate	*Determine what guidelines are applicable with minimal oversight. Apply and contribute to secure code documentation guidelines.*	
Advanced	*Develop secure coding techniques documentation. Provide guidance/supervision to others.*	

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

KSA ID	Description	Competency
K0016	Knowledge of computer programming principles	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
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Data Privacy and Protection
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
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
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	Software Development
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
S0174	Skill in using code analysis tools.	Software 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
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 18. T0022 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	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.	Core
Entry	*Under supervision, assist with documenting security controls established during the requirements phase.*	
Intermediate	*Assist in identifying key security objectives. Document security controls during the requirements phase to integrate security within the process.*	
Advanced	*Identify key security objectives. Identify security controls during the requirements phase to integrate security within the process, and to maximize software security while minimizing disruption to plans and schedules.*	

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
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
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
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture
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
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
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
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	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
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	Software Development
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
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
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 20. T0026 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.	Core
Entry	*Compile documentation of program development and subsequent revisions, referencing comments in the coded instructions so others can understand the program.*	
Intermediate	*Manage documentation of program development and subsequent revisions, reviewing comments in the coded instructions so others can understand the program.*	
Advanced	*Review and approve documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.*	

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

KSA ID	Description	Competency
K0016	Knowledge of computer programming principles	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0080	Knowledge of software design tools, methods, and techniques.	Software Development

Table 22. T0436 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Conduct trial runs of programs and software applications to ensure the desired information is produced and instructions and security levels are correct.	Core
Entry	*Assist with conducting trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.*	
Intermediate	*Conduct complex or novel trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.*	
Advanced	*Provide support/oversee trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.*	

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

KSA ID	Description	Competency
K0153	Knowledge of software quality assurance process.	Software Development
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation
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

Table 24. T0034 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.	Core
Entry	*Assist team in working with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.*	
Intermediate	*Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.*	
Advanced	*Partner with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.*	

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

KSA ID	Description	Competency
K0014	Knowledge of complex data structures.	Computer Languages
K0016	Knowledge of computer programming principles	Computer Languages
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
K0027	Knowledge of organization's enterprise information security architecture.	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
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
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
K0153	Knowledge of software quality assurance process.	Software Development
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development

Table 26. T0040 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Consult with engineering staff to evaluate interface between hardware and software.	Core
Entry	*Understand interface between hardware and software.*	
Intermediate	*Assist in evaluating interface between hardware and software. Identify constraints imposed by hardware.*	
Advanced	*Consult with engineering staff to evaluate and recommend interface between hardware and software.*	

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

KSA ID	Description	Competency
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
K0082	Knowledge of software engineering.	Software Development

Table 28. T0046 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Correct errors by making appropriate changes and rechecking the program to ensure desired results are produced.	Core
Entry	*With guidance, identify errors by making appropriate changes and rechecking the program to ensure that desired results are produced.*	
Intermediate	*Lead others to correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.*	
Advanced	*Oversee staff to train others to correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.*	

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

KSA ID	Description	Competency
K0014	Knowledge of complex data structures.	Computer Languages
K0016	Knowledge of computer programming principles	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0140	Knowledge of secure coding techniques.	Computer Languages
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
K0079	Knowledge of software debugging principles.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
K0082	Knowledge of software engineering.	Software Development
K0153	Knowledge of software quality assurance process.	Software Development
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
S0014	Skill in conducting software debugging.	Software Testing and Evaluation
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation
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

Table 30. T0057 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.	Core
Entry	*Develop and modify software systems, under direct supervision.*	
Intermediate	*Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.*	
Advanced	*Review and oversee the design, development, and modification of software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.*	

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

KSA ID	Description	Competency
K0014	Knowledge of complex data structures.	Computer Languages
K0016	Knowledge of computer programming principles	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
S0017	Skill in creating and utilizing mathematical or statistical models.	Data Analysis
A0021	Ability to use and understand complex mathematical concepts (e.g., discrete math).	Data Analysis
K0079	Knowledge of software debugging principles.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
K0082	Knowledge of software engineering.	Software Development
K0153	Knowledge of software quality assurance process.	Software Development
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development
S0014	Skill in conducting software debugging.	Software Testing and Evaluation
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	Systems Testing and Evaluation

Table 32. 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	*Assist in documenting software patches or the extent of releases that would leave software vulnerable.*	
Intermediate	*Document software patches or the extent of releases that would leave software vulnerable.*	
Advanced	*Determine and document software patches or the extent of releases that would leave software vulnerable.*	

Table 33. 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
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	Software Development
K0082	Knowledge of software engineering.	Software Development
K0153	Knowledge of software quality assurance process.	Software Development
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
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
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 34. T0077 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop secure code and error handling.	Core
Entry	*Document secure code and error handling.*	
Intermediate	*Develop secure code and error handling.*	
Advanced	*Oversee the development and definition of methods to secure code and error handling.*	

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

KSA ID	Description	Competency
K0016	Knowledge of computer programming principles	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0140	Knowledge of secure coding techniques.	Computer Languages
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	Software Development
K0079	Knowledge of software debugging principles.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development
S0014	Skill in conducting software debugging.	Software Testing and Evaluation
A0007	Ability to tailor code analysis for application-specific concerns.	Software 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
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment
K0105	Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web service description language).	Web Technology

Table 36. T0455 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop software system testing and validation procedures, programming, and documentation.	Core
Entry	*Help with developing software system testing and validation procedures, programming, and documentation.*	
Intermediate	*Develop complex or novel software system testing and validation procedures, programming, and documentation.*	
Advanced	*Oversee the development of software system testing and validation procedures, programming, and documentation.*	

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

KSA ID	Description	Competency
K0016	Knowledge of computer programming principles	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
K0079	Knowledge of software debugging principles.	Software Development
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development
S0014	Skill in conducting software debugging.	Software Testing and Evaluation
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	Systems Testing and Evaluation
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	Systems Testing and Evaluation

Table 38. T0416 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.	Core
Entry	*Support team and supervisor in using public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.*	
Intermediate	*Lead efforts to use public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.*	
Advanced	*Oversee others responsible for using public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.*	

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

KSA ID	Description	Competency
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption
K0004	Knowledge of cybersecurity and privacy principles.	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
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment

Table 40. T0100 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Core
Entry	*Follow reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.*	
Intermediate	*Recommend factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.*	
Advanced	*Review and approve factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.*	

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

KSA ID	Description	Competency
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	Systems Testing and Evaluation

Table 42. T0417 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise AV solution) when appropriate.	Core
Entry	*Support the identification of the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate.*	
Intermediate	*Identify and leverage complex or novel the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate.*	
Advanced	*Oversee the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate.*	

Table 43. 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
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
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development

Table 44. T0111 Task Analysis

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

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

KSA ID	Description	Competency
K0014	Knowledge of complex data structures.	Computer Languages
K0016	Knowledge of computer programming principles	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
S0031	Skill in developing and applying security system access controls.	Identity Management
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
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
S0014	Skill in conducting software debugging.	Software Testing and Evaluation
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation

Table 46. T0117 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development.	Core
Entry	*Identify security implications and recognize methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.*	
Intermediate	*Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.*	
Advanced	*Identify security implications and develop methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.*	

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

KSA ID	Description	Competency
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
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
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture
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
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
K0154	Knowledge of supply chain risk management standards, processes, and practices.	Risk Management

KSA ID	Description	Competency
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
S0014	Skill in conducting software debugging.	Software Testing and Evaluation
K0073	Knowledge of secure configuration management techniques. (e.g., Security Technical Implementation Guides (STIGs), cybersecurity best practices on cisecurity.org).	System Administration
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	Systems Integration
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
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment

Table 48. 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	*Under supervision, identify security issues around steady state operation and management of software and demonstrate knowledge of security measures that must be taken when a product reaches its end of life.*	
Intermediate	*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.*	
Advanced	*Identify security issues around steady state operation and management of software and create security measures that must be taken when a product reaches its end of life.*	

Table 49. 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
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
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
K0153	Knowledge of software quality assurance process.	Software Development
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation

Table 50. T0500 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.	Core
Entry	*Assist with modifying and maintaining existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.*	
Intermediate	*Modify and maintains complex, novel existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.*	
Advanced	*Oversee all modification and maintenance of existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.*	

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

KSA ID	Description	Competency
K0014	Knowledge of complex data structures.	Computer Languages
K0016	Knowledge of computer programming principles	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0140	Knowledge of secure coding techniques.	Computer Languages
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development
S0174	Skill in using code analysis tools.	Software Testing and Evaluation
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation

Table 52. T0171 Task Analysis

Proficiency		Importance
As Written within Framework	Perform integrated quality assurance testing for security functionality and resiliency attack.	Core
Entry	*Work with others to perform integrated quality assurance testing for security functionality and resiliency attack.*	
Intermediate	*Evaluate integrated quality assurance testing for security functionality and resiliency attack.*	
Advanced	*Oversee integrated quality assurance testing for security functionality and resiliency attack.*	

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

KSA ID	Description	Competency
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
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
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
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	Software Development
A0007	Ability to tailor code analysis for application-specific concerns.	Software Testing and Evaluation
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	Systems Testing and Evaluation
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	Systems Testing and Evaluation

KSA ID	Description	Competency
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	Vulnerabilities Assessment

Table 54. 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	*Demonstrate knowledge of risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.*	
Intermediate	*Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.*	
Advanced	*Plan for risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.*	

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

KSA ID	Description	Competency
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management

Table 56. T0176 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.	Core
Entry	*Under supervision, perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.*	
Intermediate	*Manage others to perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.*	
Advanced	*Coach others to perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.*	

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

KSA ID	Description	Competency
K0014	Knowledge of complex data structures.	Computer Languages
K0016	Knowledge of computer programming principles	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0140	Knowledge of secure coding techniques.	Computer Languages
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0039	Knowledge of cybersecurity and privacy principles and methods that apply to software development.	Software Development
K0079	Knowledge of software debugging principles.	Software Development
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0105	Knowledge of web services (e.g., service-oriented architecture, Simple Object Access Protocol, and web service description language).	Web Technology

Table 58. 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	*Demonstrate knowledge of 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	*Manage the storing, retrieval, and manipulation of data for analysis of system capabilities and requirements.*	

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

KSA ID	Description	Competency
K0014	Knowledge of complex data structures.	Computer Languages
K0068	Knowledge of programming language structures and logic.	Computer Languages
K0080	Knowledge of software design tools, methods, and techniques.	Software Development
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	Software Development
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment

Table 60. T0236 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	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.	Core
Entry	*Demonstrate knowledge of translating security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.*	
Intermediate	*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.*	
Advanced	*Brief others on translating security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.*	

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

KSA ID	Description	Competency
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
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
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