CAREER PATHWAY SYSTEMS SECURITY ANALYST (461)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 461-SYSTEMS SECURITY ANALYST

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 461-Systems Security Analyst.

Table 1. 461-Systems Security Analyst Work Role Overview

NICE Role Description	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.
OPM Occupational Series	Personnel performing the 461-Systems Security Analyst work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 79% - 0080-Security Administration – 6% - 1550-Computer Science – 4% - 0343-Management and Program Analysis – 3% - 0854-Computer Engineering – 2%
Work Role Pairings	Personnel performing the 461-Systems Security Analyst work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 541-Vulnerability Assessment Analyst – 14% - 451-System Administrator – 11% - 411-Technical Support Specialist – 11% - 722-Information Systems Security Manager – 9% - 612-Security Control Assessor – 8%
Functional Titles	Personnel performing the 461-Systems Security Analyst work role may unofficially or alternatively be called: - Information Assurance Specialist - Information Assurance Operational Engineer - Information Systems Security Analyst / Specialist - Network Security Vulnerability Technician (NSVT) - Information Security Analyst / Administrator - Security Analyst - Systems Analyst - Systems Security Specialist - Systems Compliance Analyst - Cybersecurity Analyst

Distribution of GS-Levels	Personnel performing the 461-Systems Security Analyst work role are most commonly found within the following grades on the General Schedule*. - ☐ GS-4 – redacted** - ☐ GS-5 – redacted** - ☐ GS-7 – redacted** - ☒ GS-9 – 3% - ☐ GS-10 – redacted** - ☒ GS-11 – 8% - ☒ GS-12 – 23% - ☒ GS-13 – 30% - ☒ GS-14 – 13% - ☒ GS-15 – 3% *21% of all 461s 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 461-Systems Security Analyst work role: - 422-Data Analyst - 441-Network Operations Specialist - 451-System Administrator - 612-Security Control Assessor - 621-Software Developer - 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 461-Systems Security Analyst work role. This is not an exhaustive list, nor does it consider learning and development opportunities an individual may pursue to prepare themselves for performing alternate work roles: - 511-Cyber Defense Analyst - 521-Cyber Defense Infrastructure Support Specialist - 531-Cyber Defense Incident Responder - 541-Vulnerability Assessment Analyst - 612-Security Control Assessor - 722-Information Systems Security Manager *Note: Leveraging the knowledge, skills, abilities, and tasks of the 461-Systems Security Analyst 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* - *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 461-Systems Security Analyst work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 461-Systems Security Analyst Core Tasks

Task ID	Task Description	Core or Additional
T0469	Analyze and report organizational security posture trends.	Core
T0470	Analyze and report system security posture trends.	Core
T0016	Apply security policies to meet security objectives of the system.	Core
T0475	Assess adequate access controls based on principles of least privilege and need-to-know.	Core
T0344	Assess all the configuration management (change configuration/release management) processes.	Core
T0309	Assess the effectiveness of security controls.	Core
T0462	Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements.	Core
T0085	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	Core
T0088	Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Core
T0485	Implement security measures to resolve vulnerabilities, mitigate risks and recommend security changes to system or system components as needed.	Core
T0489	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.	Core
T0499	Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.	Core
T0187	Plan and recommend modifications or adjustments based on exercise results or system environment.	Core
T0194	Properly document all systems security implementation, operations and maintenance activities and update as necessary.	Core
T0526	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Core
T0243	Verify and update security documentation reflecting the application/system security design features.	Core
T0508	Verify minimum security requirements are in place for all applications.	Core
T0015	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Additional
T0017	Apply service oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.	Additional
T0504	Assess and monitor cybersecurity related to system implementation and testing practices.	Additional

Task ID	Task Description	Core or Additional
T0086	Ensure application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.	Additional
T0477	Ensure the execution of disaster recovery and continuity of operations.	Additional
T0492	Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment.	Additional
T0123	Implement specific cybersecurity countermeasures for systems and/or applications.	Additional
T0128	Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.	Additional
T0169	Perform cybersecurity testing of developed applications and/or systems.	Additional
T0177	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Additional
T0548	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Additional
T0202	Provide cybersecurity guidance to leadership.	Additional
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Additional
T0545	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	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 461-Systems Security Analyst work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 461-Systems Security Analyst Core Knowledge, Skills, and Abilities

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security	Foundational to All Work Roles
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to All Work Roles
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence	Foundational to All Work Roles
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to All Work Roles
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to All Work Roles
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to All Work Roles
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense	Core
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Core
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection	Core
K0018	Knowledge of encryption algorithms.	Encryption	Core
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management	Core
S0031	Skill in developing and applying security system access controls.	Identity Management	Core

KSA ID	Description	Competency	Importance to Work Role
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Core
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management	Core
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security	Core
K0075	Knowledge of security system design tools, methods, and techniques.	Information Systems/Network Security	Core
K0276	Knowledge of security management.	Information Systems/Network Security	Core
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment	Core
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design	Core
K0322	Knowledge of embedded systems.	Infrastructure Design	Core
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design	Core
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence	Core
K0060	Knowledge of operating systems.	Operating Systems	Core
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management	Core
K0082	Knowledge of software engineering.	Software Development	Core
K0227	Knowledge of various types of computer architectures.	System Administration	Core
K0275	Knowledge of configuration management techniques.	System Administration	Core
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration	Core

KSA ID	Description	Competency	Importance to Work Role
S0024	Skill in designing the integration of hardware and software solutions.	Systems Integration	Core
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation	Core
K0093	Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).	Telecommunications	Core
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment	Core
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment	Core
S0141	Skill in assessing security systems designs.	Vulnerabilities Assessment	Core
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Vulnerabilities Assessment	Core
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	Computer Languages	Additional
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Data Privacy and Protection	Additional
K0024	Knowledge of database systems.	Database Management Systems	Additional
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption	Additional
K0285	Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.	Encryption	Additional
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture	Additional
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture	Additional
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	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

KSA ID	Description	Competency	Importance to Work Role
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
K0015	Knowledge of computer algorithms.	Mathematical Reasoning	Additional
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).	Mathematical Reasoning	Additional
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management	Additional
K0281	Knowledge of information technology (IT) service catalogues.	Operations Support	Additional
K0284	Knowledge of developing and applying user credential management system.	System Administration	Additional
K0036	Knowledge of human-computer interaction principles.	Systems Integration	Additional
K0102	Knowledge of the systems engineering process.	Systems Integration	Additional
K0266	Knowledge of how to evaluate the trustworthiness of the supplier and/or product.	Third Party Oversight/Acquisition Management	Additional
K0297	Knowledge of countermeasure design for identified security risks.	Threat Analysis	Additional
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment	Additional
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 461-Systems Security Analyst 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. 461-Systems Security Analyst Core Competencies

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Data Privacy and Protection	C014	KSAs that relate to computer network, desktop, and mainframe operating systems and their applications.	- Knowledge of Personally Identifiable Information (PII) data security standards. - Knowledge of Personal Health Information (PHI) data security standards. - Knowledge of Payment Card Industry (PCI) data security standards.	Core
Encryption	C017	KSAs that relate to the operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals.	- Knowledge of encryption algorithms - Knowledge of cryptography and cryptographic key management concepts - Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.	Core
Information Assurance	C022	KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	- Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). - Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). - Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). - Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Information Systems / Network Security	C024	KSAs that relate to the methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore security of information systems and network services.	- Knowledge of cybersecurity and privacy principles. - Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). - Knowledge of security system design tools, methods, and techniques. - Knowledge of security management. - Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Core
Systems Integration	C049	This area contains KSAs that relate to the principles, methods, and procedures for installing, integrating, and optimizing information systems components.	- Knowledge of installation, integration, and optimization of system components. - Skill in designing the integration of hardware and software solutions. - Knowledge of human-computer interaction principles. - Knowledge of the systems engineering process.	Core
Vulnerabilities Assessment	C057	KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	- Knowledge of cyber threats and vulnerabilities. - Knowledge of specific operational impacts of cybersecurity lapses. - Knowledge of how to use network analysis tools to identify vulnerabilities. - Skill in evaluating the adequacy of security designs. - Skill in assessing security systems designs. - Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning). - Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). - Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Infrastructure Design	C026	KSAs that relate to the architecture and typology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.	- Knowledge of computer networking concepts and protocols, and network security methodologies. - Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]). - Knowledge of embedded systems. - Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Additional
System Administration	C048	This area contains KSAs that relate to the upkeep, configuration, and reliable operation of computer systems.	- Knowledge of various types of computer architectures. - Knowledge of configuration management techniques. - Knowledge of developing and applying user credential management system.	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 461-Systems Security Analyst Suggested Qualifications / Capability Indicators

For indicators of capability for the 461-Systems Security Analyst 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 461-Systems Security Analyst.

2 APPENDIX: 461-SYSTEMS SECURITY ANALYST 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.

2.2 461-Systems Security Analyst Task Analysis and KSA Mapping

Table 8. T0469 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Analyze and report organizational security posture trends.	Core
Entry	*Understand baseline organizational security posture.*	
Intermediate	*Analyze and report organizational security posture trends.*	
Advanced	*Review, approve, and report organizational security posture trends, to include recommended corrective actions when necessary.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
S0031	Skill in developing and applying security system access controls.	Identity 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
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management

KSA ID	Description	Competency
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0075	Knowledge of security system design tools, methods, and techniques.	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 10. T0470 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Analyze and report system security posture trends.	Core
Entry	*Understand, track, and report deviations from baseline organizational system security posture.*	
Intermediate	*Analyze and report system security posture trends.*	
Advanced	*Review, approve, and report system security posture trends, to include recommended corrective actions when necessary.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0024	Knowledge of database systems.	Database Management Systems
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
S0141	Skill in assessing security systems designs.	Vulnerabilities Assessment
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 12. T0016 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Apply security policies to meet security objectives of the system.	Core
Entry	*Understand and apply organizational and system-specific security policies.*	
Intermediate	*Apply, [manage, and implement] security policies to meet security objectives of the system.*	
Advanced	*Approve and oversee the application of security policies to meet security objectives of the system.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0285	Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.	Encryption
S0031	Skill in developing and applying security system access controls.	Identity 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
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 14. T0475 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assess adequate access controls based on principles of least privilege and need-to-know.	Core
Entry	*Support assessment of access controls based on principles of least privilege and need-to-know.*	
Intermediate	*Assess adequate access controls based on principles of least privilege and need-to-know.*	
Advanced	*Review and approve the assessment of access controls based on principles of least privilege and need-to-know.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0024	Knowledge of database systems.	Database Management Systems
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity 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
K0275	Knowledge of configuration management techniques.	System Administration

Table 16. T0344 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assess all the configuration management (change configuration/release management) processes.	Core
Entry	*Support assessment of all the configuration management (change configuration/release management) processes.*	
Intermediate	*Assess all the configuration management (change configuration/release management) processes.*	
Advanced	*Review and approve assessment of configuration management (change configuration/release management) processes.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0024	Knowledge of database systems.	Database Management Systems
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
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
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 18. T0309 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assess the effectiveness of security controls.	Core
Entry	*Understand security controls and assist in assessing their effectiveness.*	
Intermediate	*Assess the effectiveness of security controls.*	
Advanced	*Lead, review, and/or approve the results of the assessment of the effectiveness of security controls, to include recommendations for corrective action when necessary.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 20. T0462 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements.	Core
Entry	*Observe and support fail-over tests for system operations transfer to an alternate site based on system availability requirements.*	
Intermediate	*Review procedures and [assist in testing] fail-over for system operations transfer to an alternate site based on system availability requirements.*	
Advanced	*Develop procedures and assist in testing fail-over for system operations transfer to an alternate site based on system availability requirements.*	

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

KSA ID	Description	Competency
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
S0031	Skill in developing and applying security system access controls.	Identity Management
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management

Table 22. T0085 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	Core
Entry	*Document and update security operations and maintenance activities.*	
Intermediate	*Routinely validate the proper documentation and updating of all systems security operations and maintenance activities.*	
Advanced	*Review, approve and/or report to senior leadership the status of systems security operations and maintenance activities.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0024	Knowledge of database systems.	Database Management Systems
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0275	Knowledge of configuration management techniques.	System Administration
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
S0024	Skill in designing the integration of hardware and software solutions.	Systems Integration
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
S0141	Skill in assessing security systems designs.	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 24. T0088 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Core
Entry	*Work with others to ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.*	
Intermediate	*Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.*	
Advanced	*Validate, approve, and/or report on effectiveness of cybersecurity-enabled products or other compensating security control technologies reducing identified risk to acceptable levels.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
K0285	Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.	Encryption
S0031	Skill in developing and applying security system access controls.	Identity Management
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 26. T0485 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Implement security measures to resolve vulnerabilities, mitigate risks and recommend security changes to system or system components as needed.	Core
Entry	*Assist with implementing security measures to resolve vulnerabilities and mitigate risks.*	
Intermediate	*Implement security measures to resolve vulnerabilities, mitigate risks and recommend security changes to system or system components as needed.*	
Advanced	*Oversee the implementation of security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
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
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
S0024	Skill in designing the integration of hardware and software solutions.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 28. T0489 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.	Core
Entry	*Assist with the implementation of system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.*	
Intermediate	*Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.*	
Advanced	*Oversee and make recommendations to senior leadership for system security enhancements in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.*	

Table 29. 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
K0024	Knowledge of database systems.	Database Management Systems
K0018	Knowledge of encryption algorithms	Encryption
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
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
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security

Table 30. T0499 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.	Core
Entry	*Support mitigation/correction of security deficiencies identified during security/certification testing.*	
Intermediate	*Work with system subject matter expert to mitigate/correct security deficiencies identified during security/certification testing.*	
Advanced	*Oversee the mitigation/correction of security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorizing official.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0024	Knowledge of database systems.	Database Management Systems
S0031	Skill in developing and applying security system access controls.	Identity Management
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0276	Knowledge of security management.	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
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	Risk Management
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 32. T0187 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Plan and recommend modifications or adjustments based on exercise results or system environment.	Core
Entry	*Document and provide initial analysis of exercise results or system environment.*	
Intermediate	*Plan and recommend [system security] modifications (e.g., policies, procedures, configurations, etc.) or adjustments based on exercise results or system environment.*	
Advanced	*Review, approve, and oversee implementation of recommended modifications or adjustments based on exercise results or system environment.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0024	Knowledge of database systems.	Database Management Systems
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
S0024	Skill in designing the integration of hardware and software solutions.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 34. T0194 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Properly document all systems security implementation, operations and maintenance activities and update as necessary.	Core
Entry	*Properly document all systems security implementation, operations, and maintenance activities and update as necessary.*	
Intermediate	*Evaluate all systems security implementation, operations, and maintenance activities and recommend updating as necessary.*	
Advanced	*Review and report on all systems security implementation, operations, and maintenance activities and necessary updates.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0024	Knowledge of database systems.	Database Management Systems
S0031	Skill in developing and applying security system access controls.	Identity Management
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
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Information Technology Assessment
K0036	Knowledge of human-computer interaction principles.	Systems Integration
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 36. T0526 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Core
Entry	*Provide initial data and analysis to support the drafting of cybersecurity recommendations to leadership based on significant threats and vulnerabilities.*	
Intermediate	*Draft cybersecurity recommendations to leadership based on significant threats and vulnerabilities.*	
Advanced	*Evaluate, approve, and provide cybersecurity recommendations to leadership based on significant threats and vulnerabilities.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	Enterprise Architecture
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
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0276	Knowledge of security management.	Information Systems/Network Security
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
S0141	Skill in assessing security systems designs.	Vulnerabilities Assessment

KSA ID	Description	Competency
S0167	Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment

Table 38. T0243 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Verify and update security documentation reflecting the application/system security design features.	Core
Entry	*Maintain security documentation reflecting the application/system security design features.*	
Intermediate	*Verify and update security documentation reflecting the application/system security design features.*	
Advanced	*Review and approve documented security design features of the application/system based on compliance with established regulations.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0024	Knowledge of database systems.	Database Management Systems
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0227	Knowledge of various types of computer architectures.	System Administration
K0275	Knowledge of configuration management techniques.	System Administration
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment

Table 40. T0508 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Verify minimum security requirements are in place for all applications.	Core
Entry	*Assist with verifying minimum security requirements are in place for all applications.*	
Intermediate	*Verify minimum security requirements are in place for all applications.*	
Advanced	*Review and validate that minimum security requirements are in place for all applications.*	

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

KSA ID	Description	Competency
S0147	Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).	Computer Network Defense
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0024	Knowledge of database systems.	Database Management Systems
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
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0290	Knowledge of systems security testing and evaluation methods.	Systems Testing and Evaluation
K0297	Knowledge of countermeasure design for identified security risks.	Threat Analysis
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	Vulnerabilities Assessment
S0036	Skill in evaluating the adequacy of security designs.	Vulnerabilities Assessment
S0141	Skill in assessing security systems designs.	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment