CAREER PATHWAY SECURITY ARCHITECT (652)

November 2020

5

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 652-SECURITY ARCHITECT

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 652-Security Architect.

Table 1. 652-Security Architect Work Role Overview

NICE Role Description	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.
OPM Occupational Series	Personnel performing the 652-Security Architect work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 63% - 0080-Security Administration – 11% - 1550-Computer Science – 8% - 0854-Computer Engineering – 6% - 0855-Electronics Engineering – 5%
Work Role Pairings	Personnel performing the 652-Security Architect work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 461-Systems Security Analyst – 11% - 631-Information Systems Security Developer – 11% - 641-Systems Requirements Planner– 9% - 651-Enterprise Architect – 10% - 671-System Testing and Evaluation Specialist – 6%
Functional Titles	Personnel performing the 652-Security Architect work role may unofficially or alternatively be called (Top 5 shown): - Cybersecurity Architect - Information Assurance (IA) Architect - Information Security Architect - Security Solutions Architect
Distribution of GS-Levels	Personnel performing the 652-Security Architect work role are most commonly found within the following grades on the General Schedule*. - ☐ GS-7 – redacted** - ☐ GS-9 – redacted** - ☒ GS-11 – 5% - ☒ GS-12 – 11%

	- ☒ GS-13 – 26% - ☒ GS-14 – 27% - ☒ GS-15 – 7% *26% of all 651s are in non-GS pay plans and excluded from this section **Percentages less than 3% have been redacted
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 652-Security Architect work role: - 631-Information Systems Security Developer - 632-Systems Developer - 651-Enterprise Architect - 661-Information Systems Security Developer
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 652-Security Architect 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: - 651-Enterprise Architect *Note: Leveraging the knowledge, skills, abilities, and tasks of the 212-Cyber Defense Forensics 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* - *752-Cyber Policy and Strategy Planner* - *801-Program Manager* - *901-Executive Cyber Leadership*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 652-Security Architect work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 652-Security Architect Core Tasks

Task ID	Task Description	Core or Additional
T0071	Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).	Core
T0082	Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.	Core
T0084	Employ secure configuration management processes.	Core
T0090	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	Core
T0108	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Core
T0177	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Core
T0268	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	Core
T0328	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	Core
T0484	Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.	Core
T0314	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Additional
T0307	Analyze candidate architectures, allocate security services, and select security mechanisms.	Additional
T0427	Analyze user needs and requirements to plan architecture.	Additional
T0050	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Additional
T0051	Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	Additional
T0196	Provide advice on project costs, design concepts, or design changes.	Additional
T0203	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.	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
T0338	Write detailed functional specifications that document the architecture development process.	Additional
T0448	Develop enterprise architecture or system components required to meet user needs.	Additional
T0473	Document and update as necessary all definition and architecture activities.	Additional
T0542	Translate proposed capabilities into technical requirements.	Additional

Task ID	Task Description	Core or Additional
T0556	Assess and design security management functions as related to cyberspace.	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 652-Security Architect work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 652-Security Architect Core KSAs

KSA ID	Description	Competency	Importance to Work Role
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to All Work Roles
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security	Foundational to All Work Roles
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to All Work Roles
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence	Foundational to All Work Roles
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to All Work Roles
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to All Work Roles
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.	Business Continuity	Core
A0148	Ability to serve as the primary liaison between the enterprise architect and the systems security engineer and coordinates with system owners, common control providers, and system security officers on the allocation of security controls as system-specific, hybrid, or common controls.	Client Relationship Management	Core
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	Core
K0030	Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).	Computers and Electronics	Core
K0055	Knowledge of microprocessors.	Computers and Electronics	Core
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	Data Analysis	Core
K0291	Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)	Enterprise Architecture	Core
A0061	Ability to design architectures and frameworks.	Enterprise Architecture	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

KSA ID	Description	Competency	Importance to Work Role
K0015	Knowledge of computer algorithms.	Mathematical Reasoning	Core
K0264	Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements).	Risk Management	Core
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration	Core
K0036	Knowledge of human-computer interaction principles.	Systems Integration	Core
K0071	Knowledge of remote access technology concepts.	Technology Awareness	Core
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	Telecommunications	Core
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Additional
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	Data Privacy and Protection	Additional
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection	Additional
S0374	Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations.	Data Privacy and Protection	Additional
K0024	Knowledge of database systems.	Database Management Systems	Additional
K0018	Knowledge of encryption algorithms	Encryption	Additional
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption	Additional
K0277	Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features).	Encryption	Additional
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.	Encryption	Additional
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption	Additional
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
K0293	Knowledge of integrating the organization's goals and objectives into the architecture.	Enterprise Architecture	Additional
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture	Additional
S0122	Skill in the use of design methods.	Enterprise Architecture	Additional
A0008	Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).	Enterprise Architecture	Additional
A0027	Ability to apply an organization's goals and objectives to develop and maintain architecture.	Enterprise Architecture	Additional
K0007	Knowledge of authentication, authorization, and access control methods.	Identity Management	Additional

KSA ID	Description	Competency	Importance to Work Role
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management	Additional
K0336	Knowledge of access authentication methods.	Identity Management	Additional
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance	Additional
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance	Additional
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Additional
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	Information Assurance	Additional
K0211	Knowledge of confidentiality, integrity, and availability requirements.	Information Assurance	Additional
K0240	Knowledge of multi-level security systems and cross domain solutions.	Information Assurance	Additional
S0116	Skill in designing multi-level security/cross domain solutions.	Information Assurance	Additional
S0139	Skill in applying 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
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	Information Management	Additional
K0326	Knowledge of demilitarized zones.	Information Systems/Network Security	Additional
S0076	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).	Information Systems/Network Security	Additional
S0168	Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks.	Information Systems/Network Security	Additional
S0170	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	Information Systems/Network Security	Additional
A0048	Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Additional
A0172	Ability to set up a physical or logical sub-networks that separates an internal local area network (LAN) from other untrusted networks.	Information Systems/Network Security	Additional
A0038	Ability to optimize systems to meet enterprise performance requirements.	Information Technology Assessment	Additional
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment	Additional
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	Infrastructure Design	Additional
K0057	Knowledge of network hardware devices and functions.	Infrastructure Design	Additional
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design	Additional

KSA ID	Description	Competency	Importance to Work Role
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
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design	Additional
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	Infrastructure Design	Additional
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).	Mathematical Reasoning	Additional
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	Mathematical Reasoning	Additional
S0050	Skill in design modeling and building use cases (e.g., unified modeling language).	Modeling and Simulation	Additional
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management	Additional
K0060	Knowledge of operating systems.	Operating Systems	Additional
K0320	Knowledge of organization's evaluation and validation criteria.	Organizational Awareness	Additional
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	Process Control	Additional
K0008	Knowledge of applicable business processes and operations of customer organizations.	Requirements Analysis	Additional
K0012	Knowledge of capabilities and requirements analysis.	Requirements Analysis	Additional
S0152	Skill in translating operational requirements into protection needs (i.e., security controls).	Requirements Analysis	Additional
K0214	Knowledge of the Risk Management Framework Assessment Methodology.	Risk Management	Additional
K0082	Knowledge of software engineering.	Software Development	Additional
K0286	Knowledge of N-tiered typologies (e.g. including server and client operating systems).	Software Development	Additional
A0149	Ability, in close coordination with system security officers, advise authorizing officials, chief information officers, senior information security officers, and the senior accountable official for risk management/risk executive (function), on a range of security-related issues (e.g. establishing system boundaries; assessing the severity of weaknesses and deficiencies in the system; plans of action and milestones; risk mitigation approaches; security alerts; and potential adverse effects of identified vulnerabilities).	Strategic Planning	Additional
K0227	Knowledge of various types of computer architectures.	System Administration	Additional
K0275	Knowledge of configuration management techniques.	System Administration	Additional
K0323	Knowledge of system fault tolerance methodologies.	System Administration	Additional

KSA ID	Description	Competency	Importance to Work Role
A0049	Ability to apply secure system design tools, methods and techniques.	System Administration	Additional
A0050	Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools.	System Administration	Additional
K0092	Knowledge of technology integration processes.	Systems Integration	Additional
K0102	Knowledge of the systems engineering process.	Systems Integration	Additional
S0024	Skill in designing the integration of hardware and software solutions.	Systems Integration	Additional
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation	Additional
S0061	Skill in writing test plans.	Systems Testing and Evaluation	Additional
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness	Additional
K0212	Knowledge of cybersecurity-enabled software products.	Technology Awareness	Additional
K0093	Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).	Telecommunications	Additional
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis	Additional
K0009	Knowledge of application vulnerabilities.	Vulnerabilities Assessment	Additional
K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.	Vulnerabilities Assessment	Additional
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment	Additional
A0014	Ability to communicate effectively when writing.	Written Communication	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 652-Security Architect 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. 652-Security Architect Core Competencies

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Data Privacy and Protection	C014	Relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them	• Knowledge of Personally Identifiable Information (PII) data security standards. [K0260] • Knowledge of Payment Card Industry (PCI) data security standards. [K0261] • Knowledge of Personal Health Information (PHI) data security standards. [K0262] • Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations. [S0374]	Core
Enterprise Architecture	C018	Principles, concepts, and methods of enterprise architecture to align information technology (IT) strategy, plans, and systems with the mission, goals, structure, and processes of the organization.	• Ability to apply an organization's goals and objectives to develop and maintain architecture. [A0027] • Ability to design architectures and frameworks. [A0061] • Knowledge of parallel and distributed computing concepts. [K0063] • Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]). [K0200] • Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.) [K0291] • Knowledge of integrating the organization's goals and objectives into the architecture. [K0293] • Skill in applying and incorporating information technologies into proposed solutions. [S0005]	Core
Identity Management	C020	Security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons"	• Knowledge of authentication, authorization, and access control methods. [K0007] • Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML). [K0056] • Knowledge of access authentication methods. [K0336]	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Information Assurance	C022	Methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	• Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [A0123] • Knowledge of organization's enterprise information security architecture. [K0027] • Knowledge of Security Assessment and Authorization process. [K0037] • Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [K0044] • Knowledge of key concepts in security management (e.g., Release Management, Patch Management). [K0074] • Knowledge of confidentiality, integrity, and availability requirements. [K0211] • Knowledge of multi-level security systems and cross domain solutions. [K0240] • Skill in designing multi-level security/cross domain solutions. [S0116] • Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). [S0139] • Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [S0367]	Core
Information Systems / Network Security	C024	Methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore security of information systems and network services.	• Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). [A0048] • Ability to set up a physical or logical sub-networks that separates an internal local area network (LAN) from other untrusted networks. [A0172] • Knowledge of demilitarized zones. [K0326] • Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). [S0076] • Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks. [S0168] • Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate). [S0170]	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Infrastructure Design	C026	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 capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware. [K0011] • Knowledge of network hardware devices and functions. [K0057] • 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]). [K0061] • Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. [K0170] • Knowledge of embedded systems. [K0322] • Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. [K0332] • Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs. [K0333] • Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications. [K0565]	Core
Systems Integration	C049	Principles, methods, and procedures for installing, integrating, and optimizing information systems components.	• Knowledge of installation, integration, and optimization of system components. [K0035] • Knowledge of human-computer interaction principles. [K0036] • Knowledge of technology integration processes. [K0092] • Knowledge of the systems engineering process. [K0102] • Skill in designing the integration of hardware and software solutions. [S0024]	Core
Encryption	C017	Process of transforming information to make it unreadable for unauthorized users.	• Knowledge of encryption algorithms [K0018] • Knowledge of cryptography and cryptographic key management concepts [K0019] • Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features). [K0277] • Skill in using Virtual Private Network (VPN) devices and encryption. [S0059] • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). [S0138]	Additional

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Information Technology Assessment	C025	Principles, methods, and tools (for example, surveys, system performance measures) to assess the effectiveness and practicality of information technology systems.	• Ability to optimize systems to meet enterprise performance requirements. [A0038] • Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations. [A0170] • 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. [S0027]	Additional
Mathematical Reasoning	C031	Devising strategies to solve a wide variety of math problems and determine if an assertion is correct.	• Knowledge of computer algorithms. [K0015] • Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis). [K0052] • Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression). [K0325]	Additional
Requirements Analysis	C043	Principles and methods to identify, analyze, specify, design, and manage functional and infrastructure requirements—includes translating functional requirements into technical requirements used for logical design or presenting alternative technologies or approaches.	• Knowledge of applicable business processes and operations of customer organizations. [K0008] • Knowledge of capabilities and requirements analysis. [K0012] • Skill in translating operational requirements into protection needs (i.e., security controls). [S0152]	Additional
System Administration	C048	Upkeep, configuration, and reliable operation of computer systems.	• Ability to apply secure system design tools, methods and techniques. [A0049] • Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools. [A0050] • Knowledge of various types of computer architectures. [K0227] • Knowledge of configuration management techniques. [K0275] • Knowledge of system fault tolerance methodologies. [K0323]	Additional
Technology Awareness	C053	Keeping up to date on technological developments and making effective use of technology to achieve results	• Knowledge of new and emerging information technology (IT) and cybersecurity technologies. [K0059] • Knowledge of remote access technology concepts. [K0071] • Knowledge of cybersecurity-enabled software products. [K0212]	Additional

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Vulnerabilities Assessment	C057	Principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	• Ability to conduct vulnerability scans and recognize vulnerabilities in security systems. [A0015] • Knowledge of application vulnerabilities. [K0009] • Knowledge of cyber defense and vulnerability assessment tools and their capabilities. [K0013]	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 652-Security Architect Suggested Qualifications / Capability Indicators

For indicators of capability for the 652-Security Architect 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 652-Security Architect.

2 APPENDIX: 652-SECURITY ARCHITECT 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.

2.2 652-Security Architect Task Analysis and KSA Mapping

Table 8. T0071 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).	Core
Entry	*Develop requirements for cybersecurity designs for sub-systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).*	
Intermediate	*Develop/integrate cybersecurity designs for enterprise-wide systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).*	
Advanced	*Review, approve, and integrate designs for all systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).*	

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

KSA ID	Description	Competency
A0148	Ability to serve as the primary liaison between the enterprise architect and the systems security engineer and coordinates with system owners, common control providers, and system security officers on the allocation of security controls as system-specific, hybrid, or common controls.	Client Relationship Management
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
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection
S0374	Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations.	Data Privacy and Protection
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
K0277	Knowledge of current and emerging data encryption (e.g., Column and Tablespace Encryption, file and disk encryption) security features in databases (e.g. built-in cryptographic key management features).	Encryption
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption
A0008	Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework	Enterprise Architecture

KSA ID	Description	Competency
	[TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).	
K0293	Knowledge of integrating the organization's goals and objectives into the architecture.	Enterprise Architecture
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture
S0122	Skill in the use of design methods.	Enterprise Architecture
K0007	Knowledge of authentication, authorization, and access control methods.	Identity Management
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
K0211	Knowledge of confidentiality, integrity, and availability requirements.	Information Assurance
K0240	Knowledge of multi-level security systems and cross domain solutions.	Information Assurance
S0116	Skill in designing multi-level security/cross domain solutions.	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0048	Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
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
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
K0012	Knowledge of capabilities and requirements analysis.	Requirements Analysis
S0152	Skill in translating operational requirements into protection needs (i.e., security controls).	Requirements Analysis
K0264	Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements).	Risk Management
K0286	Knowledge of N-tiered typologies (e.g. including server and client operating systems).	Software Development
A0049	Ability to apply secure system design tools, methods and techniques.	System Administration
K0227	Knowledge of various types of computer architectures.	System Administration
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0092	Knowledge of technology integration processes.	Systems Integration
K0102	Knowledge of the systems engineering process.	Systems Integration

KSA ID	Description	Competency
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0071	Knowledge of remote access technology concepts.	Technology Awareness
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	Telecommunications
S0022	Skill in designing countermeasures to identified security risks.	Threat Analysis
A0014	Ability to communicate effectively when writing.	Written Communication

Table 10. T0082 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.	Core
Entry	*Identify and document an organization's information security, cybersecurity architecture requirements, and systems security requirements throughout the acquisition life cycle.*	
Intermediate	*Analyze, decompose, and refine an organization's information security, cybersecurity architecture, and systems security requirements throughout the acquisition life cycle.*	
Advanced	*Validate and assess an organization's information security, cybersecurity architecture, and systems security requirements throughout the acquisition life cycle.*	

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

KSA ID	Description	Competency
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture
K0007	Knowledge of authentication, authorization, and access control methods.	Identity Management
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
K0336	Knowledge of access authentication methods.	Identity Management
K0211	Knowledge of confidentiality, integrity, and availability requirements.	Information Assurance
S0116	Skill in designing multi-level security/cross domain solutions.	Information Assurance
S0139	Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
A0172	Ability to set up a physical or logical sub-networks that separates an internal local area network (LAN) from other untrusted networks.	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
S0152	Skill in translating operational requirements into protection needs (i.e., security controls).	Requirements Analysis
K0082	Knowledge of software engineering.	Software Development
K0286	Knowledge of N-tiered typologies (e.g. including server and client operating systems).	Software Development
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0212	Knowledge of cybersecurity-enabled software products.	Technology Awareness

Table 12. T0084 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Employ secure configuration management processes.	Core
Entry	*Identify the changes to the architectural design in accordance with secure configuration management.*	
Intermediate	*Determine and document the impact of architectural changes in accordance with secure configuration management.*	
Advanced	*Analyze the proposed changes and update current state architecture in accordance with secure configuration management.*	

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

KSA ID	Description	Competency
K0026	Knowledge of business continuity and disaster recovery continuity of operations plans.	Business Continuity
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture
K0240	Knowledge of multi-level security systems and cross domain solutions.	Information Assurance
S0116	Skill in designing multi-level security/cross domain solutions.	Information Assurance
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0091	Knowledge of systems testing and evaluation methods.	Systems Testing and Evaluation

Table 14. T0090 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	Core
Entry	*Assess acquired or developed system(s) and architecture(s) against an organization's cybersecurity architecture guidelines.*	
Intermediate	*Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines and, if necessary, suggested corrective actions.*	
Advanced	*Validate and report on the compliance of acquired or developed system(s) and architecture(s) with organization's cybersecurity architecture guidelines.*	

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

KSA ID	Description	Competency
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection
S0005	Skill in applying and incorporating information technologies into proposed solutions.	Enterprise Architecture
S0122	Skill in the use of design methods.	Enterprise Architecture
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
K0336	Knowledge of access authentication methods.	Identity Management
K0211	Knowledge of confidentiality, integrity, and availability requirements.	Information Assurance
S0116	Skill in designing multi-level security/cross domain solutions.	Information Assurance
S0139	Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
A0048	Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0326	Knowledge of demilitarized zones.	Information Systems/Network Security
S0076	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).	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
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	Infrastructure Design
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	Network Management
S0152	Skill in translating operational requirements into protection needs (i.e., security controls).	Requirements Analysis
K0264	Knowledge of program protection planning (e.g. information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements).	Risk Management
K0082	Knowledge of software engineering.	Software Development

KSA ID	Description	Competency
A0149	Ability, in close coordination with system security officers, advise authorizing officials, chief information officers, senior information security officers, and the senior accountable official for risk management/risk executive (function), on a range of security-related issues (e.g. establishing system boundaries; assessing the severity of weaknesses and deficiencies in the system; plans of action and milestones; risk mitigation approaches; security alerts; and potential adverse effects of identified vulnerabilities).	Strategic Planning
K0323	Knowledge of system fault tolerance methodologies.	System Administration
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment

Table 16. T0108 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Core
Entry	*Document critical business functions in collaboration with organizational stakeholders.*	
Intermediate	*Identify and prioritize critical business functions in collaboration with organizational stakeholders.*	
Advanced	*Ensure critical business functions in collaboration with organizational stakeholders.*	

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

KSA ID	Description	Competency
A0008	Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).	Enterprise Architecture
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0030	Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).	Computers and Electronics
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).	Mathematical Reasoning
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
K0071	Knowledge of remote access technology concepts.	Technology Awareness
K0320	Knowledge of organization's evaluation and validation criteria.	Organizational Awareness
K0322	Knowledge of embedded systems.	Infrastructure Design

Table 18. T0177 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Core
Entry	*Gather and provide information to assist with security architecture and design reviews, gap identification in security architecture, and development of a security risk management plan.*	
Intermediate	*Perform security architecture and design reviews, identify gaps in security architecture, and provide recommendations to inform the security risk management plan.*	
Advanced	*Develop architecture review strategies and methodologies and provide leadership with recommendations to develop the security risk management plan.*	

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

KSA ID	Description	Competency
A0061	Ability to design architectures and frameworks.	Enterprise Architecture
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	Telecommunications
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	Infrastructure Design
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).	Mathematical Reasoning
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
K0063	Knowledge of parallel and distributed computing concepts.	Enterprise Architecture
K0071	Knowledge of remote access technology concepts.	Technology Awareness
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	Information Assurance
K0102	Knowledge of the systems engineering process.	Systems Integration
K0214	Knowledge of the Risk Management Framework Assessment Methodology.	Risk Management
K0240	Knowledge of multi-level security systems and cross domain solutions.	Information Assurance
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection
K0291	Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)	Enterprise Architecture

KSA ID	Description	Competency
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	Mathematical Reasoning
K0326	Knowledge of demilitarized zones.	Information Systems/Network Security
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	Infrastructure Design
S0122	Skill in the use of design methods.	Enterprise Architecture

Table 20. T0268 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	Core
Entry	*Examine how the implementation of a new system or new interfaces between systems impacts the security architecture of the current environment.*	
Intermediate	*Suggest corrective actions for addressing lapses in security resulting from new interfaces between systems.*	
Advanced	*Redesign (if needed), finalize, and codify new baseline architecture to address the impacts.*	

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

KSA ID	Description	Competency
A0048	Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
A0061	Ability to design architectures and frameworks.	Enterprise Architecture
K0007	Knowledge of authentication, authorization, and access control methods.	Identity Management
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	Telecommunications
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	Infrastructure Design
K0030	Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).	Computers and Electronics
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).	Mathematical Reasoning
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
K0057	Knowledge of network hardware devices and functions.	Infrastructure Design
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	Infrastructure Design
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	Information Assurance
K0102	Knowledge of the systems engineering process.	Systems Integration
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	Process Control

KSA ID	Description	Competency
K0211	Knowledge of confidentiality, integrity, and availability requirements.	Information Assurance
K0212	Knowledge of cybersecurity-enabled software products.	Technology Awareness
K0214	Knowledge of the Risk Management Framework Assessment Methodology.	Risk Management
K0240	Knowledge of multi-level security systems and cross domain solutions.	Information Assurance
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
K0291	Knowledge of the enterprise information technology (IT) architectural concepts and patterns (e.g., baseline, validated design, and target architectures.)	Enterprise Architecture
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.	Infrastructure Design
S0050	Skill in design modeling and building use cases (e.g., unified modeling language).	Modeling and Simulation
S0122	Skill in the use of design methods.	Enterprise Architecture
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption

Table 22. T0328 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	Core
Entry	*Identify gaps and capability changes with security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.*	
Intermediate	*Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.*	
Advanced	*Validate changes, evolve the existing architecture, and make recommendations to senior management in response to requirements contained in acquisition documents.*	

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

KSA ID	Description	Competency
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment
A0061	Ability to design architectures and frameworks.	Enterprise Architecture
K0007	Knowledge of authentication, authorization, and access control methods.	Identity Management
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	Telecommunications
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
K0024	Knowledge of database systems.	Database Management Systems
K0030	Knowledge of electrical engineering as applied to computer architecture (e.g., circuit boards, processors, chips, and computer hardware).	Computers and Electronics
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).	Mathematical Reasoning
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
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
K0071	Knowledge of remote access technology concepts.	Technology Awareness
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	Information Assurance
K0082	Knowledge of software engineering.	Software Development
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection

KSA ID	Description	Competency
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection
K0320	Knowledge of organization's evaluation and validation criteria.	Organizational Awareness
K0322	Knowledge of embedded systems.	Infrastructure Design
K0323	Knowledge of system fault tolerance methodologies.	System Administration
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	Infrastructure Design
S0050	Skill in design modeling and building use cases (e.g., unified modeling language).	Modeling and Simulation
S0122	Skill in the use of design methods.	Enterprise Architecture
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	Encryption
S0168	Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks.	Information Systems/Network Security

Table 24. T0484 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.	Core
Entry	*Support others in their efforts to determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.*	
Intermediate	*Determine the security requirements for the information system(s) and network(s) and document appropriately.*	
Advanced	*Lead determination of the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.*	

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

KSA ID	Description	Competency
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	Vulnerabilities Assessment
K0007	Knowledge of authentication, authorization, and access control methods.	Identity Management
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	Telecommunications
K0011	Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware.	Infrastructure Design
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
K0035	Knowledge of installation, integration, and optimization of system components.	Systems Integration
K0036	Knowledge of human-computer interaction principles.	Systems Integration
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance
K0052	Knowledge of mathematics (e.g. logarithms, trigonometry, linear algebra, calculus, statistics, and operational analysis).	Mathematical Reasoning
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).	Identity Management
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
K0071	Knowledge of remote access technology concepts.	Technology Awareness
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	Information Assurance
K0082	Knowledge of software engineering.	Software Development
K0102	Knowledge of the systems engineering process.	Systems Integration

KSA ID	Description	Competency
K0240	Knowledge of multi-level security systems and cross domain solutions.	Information Assurance
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
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	Mathematical Reasoning
S0122	Skill in the use of design methods.	Enterprise Architecture
S0168	Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks.	Information Systems/Network Security