CAREER PATHWAY AUTHORIZING OFFICIAL / DESIGNATING REPRESENTATIVE (611)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

CAREER PATHWAY AUTHORIZING OFFICIAL / DESIGNATING REPRESENTATIVE (611) 1

1 611-AUTHORISING OFFICIAL DESIGNATING REPRESENTATIVE 3

1.1 Work Role Overview 3

1.2 Core Tasks 5

1.3 Core Knowledge, Skills, and Abilities 6

1.4 Core Competencies 10

1.5 Suggested Qualifications / Capability Indicators 13

2 APPENDIX: 611-AUTHORIZING OFFICIAL/DESIGNATING REPRESENTATIVE TASK ANALYSIS AND KSA MAPPING 14

2.1 Key to Reading the Task Analysis and KSA Mapping 14

2.2 611- Authorizing Official/Designating Representative Task Analysis and KSA Mapping 15

1 611-AUTHORISING OFFICIAL DESIGNATING REPRESENTATIVE

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related 611-Authorizing Official/Designating Representative.

Table 1. 611-Authorizing Official/Designating Representative Work Role Overview

NICE Role Description	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).
OPM Occupational Series	Personnel performing the 611-Authorizing Official/Designating Representative work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 49% - 340-Program Management – 11% - 301-Misc. Administration and Program – 7% - 343-Management and Program Analysis – 6% - 107-Health Insurance Administration – 4%
Work Role Pairings	Personnel performing the 651-Enterprise Architect work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 801-Program Manager – 23% - 612-Security Control Assessor– 13% - 901-Execuive Cyber Leadership– 11% - 431-Knowledge Manager – 8% - 751-Cyber Workforce Developer and Manager – 8%
Functional Titles	Personnel performing the 611-Authorizing Official/Designating Representative work role may unofficially or alternatively be called: - Certifying Official - Compliance Manager - Designated Accrediting Authority - Information Assurance (IA) Officer
Distribution of GS-Levels	Personnel performing the 611-Authorizing Official/Designating Representative are most commonly found within the following grades on the General Schedule. - ☐ GS-6 – redacted* - ☐ GS-7 – redacted* - ☐ GS-9 – redacted*

	- ☐ GS-11 – redacted* - ☒ GS-12 – 7% - ☒ GS-13 – 12% - ☒ GS-14 – 16% - ☒ GS-15 – 27% *percentages less than 3% have been redacted **37% of all personnel performing the 611-Authorizing Official work role are in non-GS pay plans and excluded from this section
On Ramps	The following work roles are examples of logical roles an individual may perform prior to transitioning into the 611-Authorizing Official/Designating Representative work role: - 752-Cyber Policy and Strategy Planner - 801-Program Manager - 901-Executive Cyber Leadership
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 611-Authorizing Official. 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: - 752-Cyber Policy and Strategy Planner - 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 611-Authorizing Official/Designating Representative work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 611- Authorizing Official/Designating Representative Core Tasks

Task ID	Task	Core or Additional
T0145	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Core
T0221	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Core
T0371	Establish acceptable limits for the software application, network, or system.	Core
T0495	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Core

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 611-Authorizing Official/Designating Representative work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 611- Authorizing Official/Designating Representative Core KSAs

KSA ID	Description	Competency	Importance to Work Role
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	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
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to All Work Roles
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to All Work Roles
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	Data Privacy and Protection	Core
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance	Core
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance	Core
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance	Core
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Core
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT)	Information Assurance	Core

KSA ID	Description	Competency	Importance to Work Role
	security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.		
K0295	Knowledge of confidentiality, integrity, and availability principles.	Information Assurance	Core
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Core
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security	Core
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence	Core
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management	Core
K0084	Knowledge of structured analysis principles and methods.	Risk Management	Core
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management	Core
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness	Core
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement	Additional
A0111	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.	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
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration	Additional
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption	Additional
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture	Additional

KSA ID	Description	Competency	Importance to Work Role
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	Enterprise Architecture	Additional
A0090	Ability to identify external partners with common cyber operations interests.	External Awareness	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
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance	Additional
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security	Additional
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment	Additional
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
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	Legal, Government, and Jurisprudence	Additional
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence	Additional
A0077	Ability to coordinate cyber operations with other organization functions or support activities.	Operations Support	Additional
A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.	Organizational Awareness	Additional
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.	Organizational Awareness	Additional

KSA ID	Description	Competency	Importance to Work Role
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	Organizational Awareness	Additional
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness	Additional
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management	Additional
A0028	Ability to assess and forecast manpower requirements to meet organizational objectives.	Strategic Planning	Additional
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation	Additional
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	Systems Testing and Evaluation	Additional
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional
K0013	Knowledge of cyber defense and vulnerability assessment tools and their capabilities.	Vulnerabilities Assessment	Additional
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment	Additional
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment	Additional
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 611-Authorizing Official/Designating Representative 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. 611- Authorizing Official/Designating Representative 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 Personal Health Information (PHI) data security standards. [K0262] - Ability to work across departments and business units to implement organization's privacy principles and programs and align privacy objectives with security objectives. [A0111] - Knowledge of Payment Card Industry (PCI) data security standards. [K0261]	Core
Information Assurance	C022	Methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	- Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). [K0203] - Knowledge of organization's enterprise information security architecture. [K0101] - Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [A0123] - Knowledge of confidentiality, integrity, and availability principles. [K0295] - Knowledge of Security Assessment and Authorization process. [K0037] - Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities. [K0054] - Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [S0367] - Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). [K0044] - Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data. [K0038]	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
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.	- Skill in discerning the protection needs (i.e., security controls) of information systems and networks. [S0034] - Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). [K0179] - Knowledge of cybersecurity and privacy principles. [K0004] - Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). [K0049]	Core
Legal, Government, and Jurisprudence	C030	Laws, regulations, policies, and ethics that can impact organizational activities.	- Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. [K0003] - Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures. [K0267] - Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives. [A0094] - Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. [K0168]	Core
Organizational Awareness	C037	Understanding an organization's mission and functions, its social and political structure and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization.	- Knowledge of the organization's core business/mission processes. [K0146] - Ability to understand the basic concepts and issues related to cyber and its organizational impact. [A0119] - Ability to relate strategy, business, and technology in the context of organizational dynamics. [A0117] - Ability to understand technology, management, and leadership issues related to organization processes and problem solving. [A0118]	Core
Risk Management	C044	Methods and tools used for risk assessment and mitigation of risk.	- Knowledge of structured analysis principles and methods. [K0084] - Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). [K0002] - Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures. [K0169] - Knowledge of Risk Management Framework (RMF) requirements. [K0048]	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 computer networking concepts and protocols, and network security methodologies. [K0001] - Knowledge of embedded systems. [K0322] - Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations. [K0170]	Additional
Vulnerabilities Assessment	C057	Principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	- Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list). [K0624] - Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). [K0070] - Knowledge of specific operational impacts of cybersecurity lapses. [K0006] - Knowledge of cyber defense and vulnerability assessment tools and their capabilities. [K0013] - Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins). [K0040] - Knowledge of cyber threats and vulnerabilities. [K0005] - Knowledge of penetration testing principles, tools, and techniques. [K0342]	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 611-Authorizing Official/Designating Representative Suggested Qualifications / Capability Indicators

For indicators of capability for the 611-Authorizing Official 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 611-Authorizing Official.

2 APPENDIX: 611-AUTHORIZING OFFICIAL/DESIGNATING REPRESENTATIVE 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.

2.2 611- AUTHORIZING OFFICIAL/DESIGNATING REPRESENTATIVE TASK ANALYSIS AND KSA MAPPING

Table 8. T0145 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Core
Entry	*Review accreditation packages and make accreditation recommendation.*	
Intermediate	*Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).*	
Advanced	*Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2) and make recommendations for improvement in the packages.*	

Table 9. 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
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection
A0111	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.	Data Privacy and Protection
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0295	Knowledge of confidentiality, integrity, and availability principles.	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design

KSA ID	Description	Competency
K0322	Knowledge of embedded systems.	Infrastructure Design
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	Legal, Government, and Jurisprudence
A0077	Ability to coordinate cyber operations with other organization functions or support activities.	Operations Support
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.	Organizational Awareness
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.	Organizational Awareness
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	Organizational Awareness
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 10. T0221 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Core
Entry	*Support the review of authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.*	
Intermediate	*Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.*	
Advanced	*Lead reviewers of authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.*	

Table 11. 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
K0262	Knowledge of Personal Health Information (PHI) data security standards.	Data Privacy and Protection
A0111	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.	Data Privacy and Protection
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Enterprise Architecture
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance
K0038	Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0295	Knowledge of confidentiality, integrity, and availability principles.	Information Assurance
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
A0170	Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.	Information Technology Assessment
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design
K0322	Knowledge of embedded systems.	Infrastructure Design

KSA ID	Description	Competency
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence
A0077	Ability to coordinate cyber operations with other organization functions or support activities.	Operations Support
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.	Organizational Awareness
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.	Organizational Awareness
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	Organizational Awareness
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management
K0048	Knowledge of Risk Management Framework (RMF) requirements.	Risk Management
K0084	Knowledge of structured analysis principles and methods.	Risk Management
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 12. T0371 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Establish acceptable limits for the software application, network, or system.	Core
Entry	*Recommend acceptable limits for the software application, network, or system.*	
Intermediate	*Establish acceptable limits for the software application, network, or system.*	
Advanced	*Continuously refine acceptable limits for the software application, network, or system.*	

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

KSA ID	Description	Competency
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement
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
A0111	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.	Data Privacy and Protection
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
K0295	Knowledge of confidentiality, integrity, and availability principles.	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence

KSA ID	Description	Competency
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	Legal, Government, and Jurisprudence
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.	Organizational Awareness
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.	Organizational Awareness
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	Organizational Awareness
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	Systems Testing and Evaluation
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment

Table 14. T0495 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Core
Entry	*Assist in management of Accreditation Packages (e.g., ISO/IEC 15026-2).*	
Intermediate	*Manage Accreditation Packages (e.g., ISO/IEC 15026-2).*	
Advanced	*Lead those managing Accreditation Packages (e.g., ISO/IEC 15026-2).*	

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

KSA ID	Description	Competency
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)	Contracting/Procurement
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
A0111	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.	Data Privacy and Protection
K0622	Knowledge of controls related to the use, processing, storage, and transmission of data.	Database Administration
K0019	Knowledge of cryptography and cryptographic key management concepts	Encryption
K0027	Knowledge of organization's enterprise information security architecture.	Information Assurance
K0037	Knowledge of Security Assessment and Authorization process.	Information Assurance
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	Information Assurance
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	Information Assurance
K0295	Knowledge of confidentiality, integrity, and availability principles.	Information Assurance
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	Information Systems/Network Security
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Information Systems/Network Security
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design
K0170	Knowledge of critical infrastructure systems with information communication technology that were designed without system security considerations.	Infrastructure Design
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	Legal, Government, and Jurisprudence
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	Legal, Government, and Jurisprudence

KSA ID	Description	Competency
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	Legal, Government, and Jurisprudence
K0146	Knowledge of the organization's core business/mission processes.	Organizational Awareness
A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.	Organizational Awareness
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.	Organizational Awareness
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	Organizational Awareness
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	Policy Management
K0169	Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures.	Risk Management
K0028	Knowledge of organization's evaluation and validation requirements.	Systems Testing and Evaluation
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	Systems Testing and Evaluation
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	Technology Awareness
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment
K0040	Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).	Vulnerabilities Assessment
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	Vulnerabilities Assessment
K0342	Knowledge of penetration testing principles, tools, and techniques.	Vulnerabilities Assessment