CAREER PATHWAY CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST (521)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 521-CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 521-Cyber Defense Infrastructure Support Specialist.

Table 1. 521-Cyber Defense Infrastructure Support Specialist Work Role Overview

NICE Role Description	Tests, implements, deploys, maintains, and administers infrastructure hardware and software.
OPM Occupational Series	Personnel performing the 521-Cyber Defense Infrastructure Support Specialist work role are most commonly aligned to the following Occupational Series (Top 5 shown): - 2210-Information Technology – 79% - 2504-Wire Communications Cable Splicing – 5% - 391-Telecommunications – 5% - 1550-Computer Science – 3% - 0855-Electronics Engineering – 3%
Work Role Pairings	Personnel performing the 521-Cyber Defense Infrastructure Support Specialist work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 541-Vulnerability Assessment Analyst - 19% - 451-System Administrator – 16% - 411-Technical Support Specialist – 13% - 441-Network Operations Specialist – 12% - 531-Cyber Defense Incident Responder – 10%
Functional Titles	Personnel performing the 521-Cyber Defense Infrastructure Support Specialist work role may unofficially or alternatively be called: - Continuous Diagnostics and Mitigation Specialist - Continuous Monitoring Specialist - Cyber Defense Engineer / Administrator - Cyber Tool Engineer / Administrator - Disaster Recovery / Emergency Management Specialist - Intrusion Detection System Administrator / Technician - Network Security Specialist / Engineer - Systems Security Administrator / Engineer - Trusted Internet Connection (TIC) Gateway Engineer
Distribution of GS-Levels	Personnel performing the 521-Cyber Defense Infrastructure Support Specialist work role are most commonly found within the following grades on the General Schedule*. - ☐ GS-5 – redacted** - ☐ GS-7 – redacted** - ☒ GS-9 – 7%

	- ☐ GS-10 – redacted** - ☒ GS-11 – 13% - ☒ GS-12 – 26% - ☒ GS-13 – 28% - ☒ GS-14 – 13% - ☐ GS-15 – redacted** *23% of all 521s are in non-GS pay plans and excluded from this section **Percentages below 3% are redacted.
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 521-Cyber Defense Infrastructure Support Specialist work role: - 441-Network Operations Specialist - 451-System Administrator - 461-Systems Security Analyst - 511-Cyber Defense Analyst - 671-System Testing and Evaluation Specialist
Off Ramps	The following work roles are examples of common transitions an individual may pursue after having performed the 521-Cyber Defense Infrastructure Support Specialist. 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: - 212-Cyber Defense Forensics Analyst - 531-Cyber Defense Incident Responder - 541-Vulnerability Assessment Analyst - 722-Information Systems Security Manager *Note: Leveraging the knowledge, skills, abilities, and tasks of the 521-Cyber Defense Infrastructure Support Specialist work role, individuals may prepare themselves to transition into one or more of the following cross-functional work roles: - *711- Cyber Instructional Curriculum Developer* - *712-Cyber Instructor* - *751-Cyber Workforce Developer and Manager* - *752-Cyber Policy and Strategy Planner* - *802-IT Project Manager* - *803-Product Support Manager*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 521-Cyber Defense Infrastructure Support Specialist work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 521-Cyber Defense Infrastructure Support Specialist Core Tasks

Task ID	Task	Core or Additional
T0261	Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.	Core
T0335	Build, install, configure, and test dedicated cyber defense hardware.	Core
T0420	Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).	Core
T0438	Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).	Core
T0483	Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).	Core
T0486	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.	Core
T0042	Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.	Additional
T0180	Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.	Additional
T0348	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.	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 521-Cyber Defense Infrastructure Support Specialist work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 521-Cyber Defense Infrastructure Support Specialist Core Knowledge, Skills, and Abilities

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity and privacy principles.	Information Systems/Network Security	Foundational to All Work Roles
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
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense	Core
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense	Core
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	Computer Network Defense	Core
K0104	Knowledge of Virtual Private Network (VPN) security.	Encryption	Core
K0042	Knowledge of incident response and handling methodologies.	Incident Management	Core
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance	Core
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security	Core
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security	Core
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Core
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design	Core
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).	Network Management	Core
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).	Process Control	Core

KSA ID	Description	Competency	Importance to Work Role
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment	Core
K0021	Knowledge of data backup and recovery.	Business Continuity	Additional
S0053	Skill in tuning sensors.	Computer Network Defense	Additional
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	Computer Network Defense	Additional
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.	Encryption	Additional
S0054	Skill in using incident handling methodologies.	Incident Management	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
S0007	Skill in applying host/network access controls (e.g., access control list).	Information Systems/Network Security	Additional
S0077	Skill in securing network communications.	Information Systems/Network Security	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
K0058	Knowledge of network traffic analysis methods.	Network Management	Additional
K0205	Knowledge of basic system, network, and OS hardening techniques.	System Administration	Additional
S0121	Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).	System Administration	Additional
K0274	Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.	Telecommunications	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 521-Cyber Defense Infrastructure Support Specialist 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. 521-Cyber Defense Infrastructure Support Specialist Core Competencies

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Computer Network Defense	C007	KSAs that relate to the defensive measures to detect, respond, and protect information, information systems, and networks from threats.	- Knowledge of cyber defense and information security policies, procedures, and regulations. - Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications. - Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	Core
Information Assurance	C022	KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	- Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). - Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). - Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Core
Information Systems / Network Security	C024	KSAs that relate to the methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore security of information systems and network services.	- Knowledge of cybersecurity and privacy principles. - Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists). - Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). - Skill in applying host/network access controls (e.g., access control list). - Skill in securing network communications.	Core

Technical Competency	Comp ID	Definition	Work Role Related KSAs	Importance
Infrastructure Design	C026	KSAs that relate to the architecture and typology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software.	- Knowledge of computer networking concepts and protocols, and network security methodologies. - Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. - 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]).	Core
Vulnerabilities Assessment	C057	KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	- Knowledge of cyber threats and vulnerabilities. - Knowledge of specific operational impacts of cybersecurity lapses. - Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. - Knowledge of packet-level analysis.	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 521-Cyber Defense Infrastructure Support Specialist Suggested Qualifications / Capability Indicators

For indicators of capability for the 521-Cyber Defense Infrastructure Support Specialist 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 521-Cyber Defense Infrastructure Support Specialist.

2 APPENDIX: 521-CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST 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.

2.2 521-Cyber Defense Infrastructure Support Specialist Task Analysis and KSA Mapping

Table 8. T0042 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Coordinate with Cyber Defense Analysts to administer existing rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications, including responding to alerts.	Core
Entry	*Coordinate with Cyber Defense Analysts to administer existing rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications, including responding to alerts.*	
Intermediate	*Coordinate with Cyber Defense Analysts to administer existing rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications, including responding to alerts.*	
Advanced	*Coordinate with Cyber Defense Analysts to administer existing rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications, including responding to alerts.*	

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

KSA ID	Description	Competency
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0058	Knowledge of network traffic analysis methods.	Network 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
K0135	Knowledge of web filtering technologies.	Web Technology
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
S0007	Skill in applying host/network access controls (e.g., access control list).	Information Systems/Network Security
S0053	Skill in tuning sensors.	Computer Network Defense

S0077	Skill in securing network communications.	Information Systems/Network Security
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	Computer Network Defense
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	Computer Network Defense

Table 10. T0180 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.	Core
Entry	*Under supervision, install and configure specialized cyber defense applications, systems (e.g., antivirus, audit and remediation) and hardware devices, to include maintenance, backup, and restoration.*	
Intermediate	*Perform system administration on specialized cyber defense applications, systems (e.g., antivirus, audit and remediation) and hardware devices, to include installation, configuration, maintenance, backup, and restoration.*	
Advanced	*Oversee the administration and integration of specialized cyber defense applications and systems, while serving as an escalation point of contact for the organization.*	

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

KSA ID	Description	Competency
K0021	Knowledge of data backup and recovery.	Business Continuity
K0104	Knowledge of Virtual Private Network (VPN) security.	Encryption
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0205	Knowledge of basic system, network, and OS hardening techniques.	System Administration
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).	Process Control
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
S0007	Skill in applying host/network access controls (e.g., access control list).	Information Systems/Network Security
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.	Encryption
S0077	Skill in securing network communications.	Information Systems/Network Security
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	Computer Network Defense

Table 12. T0261 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.	Core
Entry	*Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.*	
Intermediate	*Coordinate identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.*	
Advanced	*Lead the identification, prioritization, and coordination the protection of critical cyber defense infrastructure and key resources.*	

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

KSA ID	Description	Competency
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).	Process Control
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).	Network Management
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	Computer Network Defense
S0367	Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance

Table 14. T0335 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Build, install, configure, and test dedicated cyber defense hardware.	Core
Entry	*Build, install, configure, and test dedicated cyber defense hardware using existing SOPs.*	
Intermediate	*Build, install, configure, and test new configurations of dedicated cyber defense hardware and modify existing and or create new SOPs.*	
Advanced	*Overseeing and resolving complex designs, builds, installation, configuration, and testing dedicated cyber defense hardware, while modifying and approving existing or creating new SOPs.*	

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

KSA ID	Description	Competency
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0104	Knowledge of Virtual Private Network (VPN) security.	Encryption
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).	Process Control
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).	Network Management
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	Computer Network Defense
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	Computer Network Defense

Table 16. T0348 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.	Core
Entry	*Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.*	
Intermediate	*Assess the impact of implementing and sustaining a dedicated cyber defense infrastructure.*	
Advanced	*Lead the assessment and oversee the impact of implementing and sustaining a dedicated cyber defense infrastructure.*	

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

KSA ID	Description	Competency
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0042	Knowledge of incident response and handling methodologies.	Incident Management
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
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
K0104	Knowledge of Virtual Private Network (VPN) security.	Encryption
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).	Process Control
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).	Network Management
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	Computer Network Defense

S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	Computer Network Defense

Table 18. T0420 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).	Core
Entry	*Assist with the administration test bed(s), to test and evaluate cyber defense infrastructure (e.g. applications, hardware infrastructure, virtualized environments, rules/signatures, access controls, and configurations of platforms), referencing SOPs as necessary.*	
Intermediate	*Administer test bed(s) to test and evaluate cyber defense infrastructure (e.g. applications, hardware infrastructure, virtualized environments, rules/signatures, access controls, configurations of platforms).*	
Advanced	*Oversee others administrating test bed(s), to test and evaluate cyber defense infrastructure, (e.g. applications, hardware infrastructure, virtualized environments rules/signatures, access controls, and configurations of platforms), briefing leadership on the results as necessary.*	

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

KSA ID	Description	Competency
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
S0079	Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).	Computer Network Defense
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	Computer Network Defense
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.	Encryption
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	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
S0077	Skill in securing network communications.	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
K0058	Knowledge of network traffic analysis methods.	Network Management

K0334	Knowledge of network traffic analysis (tools, methodologies, processes).	Network Management
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).	Process Control
S0121	Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).	System Administration
K0062	Knowledge of packet-level analysis.	Vulnerabilities Assessment
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment

Table 20. T0438 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).	Core
Entry	*Assist with modifying network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).*	
Intermediate	*Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).*	
Advanced	*Oversee the creation, editing, management, and approvals of network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems), to include troubleshooting and escalation as required.*	

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

KSA ID	Description	Competency
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0058	Knowledge of network traffic analysis methods.	Network 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
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).	Process Control
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).	Network Management
S0007	Skill in applying host/network access controls (e.g., access control list).	Information Systems/Network Security

S0077	Skill in securing network communications.	Information Systems/Network Security
S0121	Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).	System Administration
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	Computer Network Defense

Table 22. T0483 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).	Core
Entry	*Support the identification of conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).*	
Intermediate	*Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).*	
Advanced	*Oversee the identification and remediation of conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).*	

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

KSA ID	Description	Competency
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0058	Knowledge of network traffic analysis methods.	Network 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
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).	Process Control
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design
S0053	Skill in tuning sensors.	Computer Network Defense
S0077	Skill in securing network communications.	Information Systems/Network Security
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	Computer Network Defense

Table 24. T0486 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.	Core
Entry	*Assist with the implementation of Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the area of responsibility, maintaining records as needed.*	
Intermediate	*Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the area of responsibility, maintaining records as needed.*	
Advanced	*Oversee and approve the implementation of Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the area of responsibility, maintaining records as needed.*	

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

KSA ID	Description	Competency
K0021	Knowledge of data backup and recovery.	Business Continuity
K0033	Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).	Information Systems/Network Security
K0044	Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	Information Assurance
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
K0106	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.	Vulnerabilities Assessment
K0157	Knowledge of cyber defense and information security policies, procedures, and regulations.	Computer Network Defense
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	Information Systems/Network Security
K0205	Knowledge of basic system, network, and OS hardening techniques.	System Administration
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	Computer Network Defense
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	Infrastructure Design

S0121	Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.).	System Administration
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