| Occupation: Cyber Sec | urity Support Technicia | n | ONET Code 1: | 5-1122 | |
|---|---|--|---|---|------------------|
| | | | RAPIDS Code | : | |
| OCCUPATIONAL OVER | RVIEW | | | | |
| Potential Job Titles: Cyber network security analyst | security analyst, cyber so | ecurity monitor, vulnerabi | lity analyst, information systems | s security analyst, | |
| | | | e employees of small to large cor organizations, and can be self-e | | |
| networks and devices. Acco | ording to the National Cy tions: securely provision, | bersecurity Workforce Fra | rity and integrity of information amework, cyber security profess steet and defend, investigate, col | ionals perform on | e or |
| Occupational Pathways: Cy | ber security support tech | | and additional certifications, can systems security manager and inf | | |
| solve complex problems an | d work with a wide range ipment and systems. Th | e of people, including other ese individuals also need to | riented, enjoy working with tecer technical staff as well as non-to have patience and be able to r | technical uses of | _ |
| Certification or Licensure: CompTia Security+ (Certification Certified Information Syste Professional (CISSP) (Certification) | ms Security | certification opportunitie enable an individual to co their career. Among thos | as: Multiple software and hardware to demonstrate a wide range of ontinue expanding their knowledge vendors and organizations wells are: CompTIA, Cisco, Micros | f competencies an dge and skills thro ll known to provice | d that ughout |
| Large Employers | Trade Associations | | Regulatory Agencies Department of Homeland Secur National Institute of Standards a Department of Defense Department of Treasury | | |
| Number of current employe | ees (2014-2024): 85,000 | | Endard Rurani at Invactigation | | |
| Number of additional job of | penings predicted (2014 | -2024): 25,500 | | | |
| Median Salary (2014): \$67, | , , , , , | * | | | |
| Job Function 1: Assists in d compliance with network se | | | n enforcing company | | |
| Job Function 2: Provides to | echnical support to users | or customers | | | |
| Job Function 3: Installs, co including hardware and sof | | | | | |
| Job Function 4: Installs, co confidentiality, integrity and vulnerability management. | d availability; also manag | ges accounts, firewalls, co | nfiguration, patch and | | |
| Job Function 5: Configures | s tools and technologies t | o detect, mitigate and prev | vent potential threats | | |
| Job Function 6: Assesses a vulnerabilities | nd mitigates system netw | vork, business continuity a | nd related security risks and | | |
| Job Function 7: Reviews notential threats | etwork utilization data to | identify unusual patterns, | suspicious activity or signs of | | |
| Job Function 8: Responds | to cyber intrusions and at | ttacks and provides defens | ive strategies | | |
| | | | | | |

| l Effectiveness Competen | nies | | | | | | | | |
|---|------|---|---|---|---|---|---|---|---------|
| i Effectiveness Competen | cies | | | | | | | | |
| Relevance (Using Lumina Beta Credentials Framework | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Interpersonal Skills | | X | | | | | | | + |
| Integrity | | | | | X | | | | + |
| Professionalism | | | | | X | | | | |
| Initiative | | | X | | | | | | |
| Reliability | | | | | X | | | | |
| Dependability & Reliability | | | | | X | | | | |
| Adaptability & Flexibility | | | X | | | | | | |
| Lifelong Learning | | | | | X | | | | |
| ic Competencies | | | | | | | | | |
| Relevance (Based on Lumina Beta Credentials Framework | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Reading | | | X | | | | | | |
| Writing | | | X | | | | | | |
| Mathematics | | | | | X | | | | |
| Science & Technology | | | | | X | | | | |
| Communication | | | X | | | | | | |
| Critical & Analytical Thinking | | | | | X | | | | |
| | | | | | X | | | | \perp |
| Basic Computer Skills | | | | | | | | | |
| ace Competencies | | | | 2 | 4 | 5 | 6 | 7 | 8 |
| | 0 | 1 | 2 | 3 | | | | | |
| Relevance (Based on Lumina Beta | | 1 | 2 | 3 | X | | | | + |

| Creative Thinking | | | | X | | | |
|--------------------------------------|---|---|---|---|---|--|--|
| Problem Solving & Decision Making | | | | | X | | |
| Working with Tools & Technology | | | | | X | | |
| Scheduling & Coordinating | | | X | | | | |
| Checking, Examining & Recording | | | | | X | | |
| Business Fundamentals | | X | | | | | |
| Sustainable Practices | X | | | | | | |
| Health & Safety | | X | | | | | |

| Certifications | |
|---|--|
| CompTia Security+ (Certification) | |
| Certified Information Systems Security Professional (CISSP) (Certification) | |
| Multiple Vendor Certifications available, such as CISCO, | |
| | |
| | |
| | |
| | |
| description | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

| WORK PROCESS SCHEDULE | Cyber Se | ecurity | | | ONET Code 15- | .1122.00 | |
|--|------------------|------------|------------|-------------------|---|--|--|
| Support Technician | | | | | RAPIDS Code | | |
| Job Title | | | _ | | | | |
| | | | | | | | |
| Company Contact: | | | | | | | |
| Apprenticeship Type: (competency based, time based, hybrid) | | | | | | | |
| Minimum Time Requirements (or time range): | | | | | | | |
| Required Certifications: CompTIA A+ (many other certifications are | available includ | ing vendor | certificat | ions) Certif | ied Information Sv | stems Security | |
| Professional (CISSP) is another core certification, but it does require curring the apprenticeship program. | | | | | | | |
| JOB FUNCTION | | | | | | | |
| JOB FUNCTION 1: Assists in developing security policies and protocols; assists in enfor company compliance with network security policies and protocols | reing | | | LEVEL | NICE Framework Category | NICE Framework Specialty Area | |
| Competency 1a: Locates (in Intranet, employee handbook or security protocols) organiza policies intended to maintain security and minimize risk and explains their use | tional | | | Basic | Oversee and Govern | Education and Training | |
| Competency 1b: Provides guidance to employees on how to access networks, set passwor reduce security threats and provide defensive measures associated with searches, software downloads, email, Internet, add-ons, software coding and transferred files | | | | Dasic | Oversee and Govern | Hammig | |
| Comparing to 10. Facures that recovered show staristics are supplied and anfarced and the | * | | | Advanced | Securely Provision | Information Assurance Compliance | |
| Competency 1c: Ensures that password characteristics are explained and enforced and the updates are required and enforced based on appropriate time intervals | 11 | | | Basic | Securely Provision | Information Assurance Compliance | |
| Competency 1d: Explains company or organization's policies regarding the storage, use a transfer of sensitive data, including intellectual property and personally identifiable inform Identifies data life cycle, data storage facilities, technologies and describes business continisks | | | | | | Education and | |
| Competency 1e: Assigns individuals to the appropriate permission or access level to contraccess to certain web IP addresses, information and the ability to download programs and data to various locations | transfer | | | Advanced Advanced | Oversee and Govern Securely Provision | Training Information Assurance Compliance | |
| Competency 1f: Assists employees in the use of technologies that restrict or allow for ren access to the organization's information technology network | note | | | Intermediate | Oversee and Develop | Education and Training | |
| Competency 1g: Develops security compliance policies and protocols for external service Cloud service providers, software services, external data centers) | es (i.e. | | | Advanced | Securely provision | Information Assurance Compliance | |
| Completency 1h: Complies with incident response and handling methodologies | | | | Advanced | Protect and Defend | Computer Network Defense Analysis | |
| Competency 1i: Articulates the business need or mission of the organization as it pertains use of IT systems and the storage of sensitive data | to the | | | Intermediate | Securely Provision | System Security Architecture | |
| JOB FUNCTION 2: Provides technical support to users or customers | | | | | | | |
| Competency 2a: Manages inventory of IT resources | | | | Basic | Operate/Maintain - | Customer Service and Technical Support | |
| Competency 2b: Diagnoses and resolves customer-reported system incidents | | | | Intermediate | Investigate | Digital forensics | |
| Competency 2c: Installs and configures hardware, software and peripheral equipment for users | system | | | Basic | Operate and Maintain | Customer service Technical support | |
| Competency 2d: Monitors client-level computer system performance | | | | Basic | | Customer service | |
| Competency 2e: Tests computer system performance | | | | Basic | Operate and Maintain Operate and Maintain | Customer Service and Technical Support | |
| Competency 2f: Troubleshoots system hardware and software | | | | Basic | Operate and Maintain | Customer Service and Technical Support | |
| Competency 2g: Administers accounts, network rights, and access to systems and equipment of the competency 2g: Administers accounts, network rights, and access to systems and equipment of the competency 2g: Administers accounts, network rights, and access to systems and equipment of the competency 2g: Administers accounts, network rights, and access to systems and equipment of the competency 2g: Administers accounts, network rights, and access to systems and equipment of the competency 2g: Administers accounts, network rights, and access to systems and equipment of the competency 2g: Administers accounts and access to systems and equipment of the competency 2g: Administer access to systems and equipment of the competency 2g: Administer access to systems and equipment of the competency 2g: Administer access to systems and access to systems access to systems and access to systems acc | nent | | | Intermediate | Operate and Maintain | Customer Service and Technical Support | |
| Competency 2h: Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines | | | | Advanced | Operate and Maintain | Systems Security Analysis | |
| JOB FUNCTION 3: Installs, configures, tests, operates, maintains and manages networks their firewalls including hardware and software that permit sharing and transmission of information | | | | | | | |
| Competency 3a: Collaborates with system developers and users to assist in the selection of appropriate design solutions to ensure the compatibility of system components | | | | Intermediate | Securely Provision | Systems Security Architecture | |
| Competency 3b: Installs, replaces, configures and optimizes network hubs, routers and sw | vitches | | | Advanced | Operate and Maintain | Network Services | |

| Lienmentant (Propose part Annexes the processor) Comprising SA Tologous in throwing pollutions Comprising SA Tologous returned controlling pollutions Comprising SA Tologous returned pollutions C | | | | | | |
|--|---|----|--------------|----------------------|------------------|--|
| Sequences of the Marines returns infrastructure to server one purpose or improve workflow Computersy 3° Indigents now systems since versing network architecture Computersy 3° Indigents now systems since versing network architecture Computersy 3° Indigents now systems since versing network architecture Computersy 3° Indigents now systems since versing network architecture Computersy 3° Indigents now systems since versing network architecture Computersy 3° Indigents now systems since versing network architecture Computersy 3° Indigents now systems since versing network architecture Computersy 3° Indigents now systems since versing network architecture Computersy 3° Indigents now systems since versing network architecture Computersy 3° Indigents now systems and surprise of losse provides and furnishment of the system and surprise of losse provides and surprise of losses | Competency 3c: Assists in network backup and recovery procedures | | Intermediate | Operate and Maintain | Network Services | |
| Advanced Operate and Maintain Secretic Services in Secreting services and recommendations of the commendation of the commendat | Competency 3d: Diagnoses network connectivity problems | | Basic | Operate and Maintain | Network Services | |
| Competency See Patients network valuarabilities to sensure information is subgraued against Competency See Repairs network valuarabilities to sensure information is subgraued against Competency See Repairs network valuarabilities to sensure information in the competency of the competency See Repairs network valuarabilities contained to the competency of the competency See Repairs network valuarabilities of the competency See Repairs network valuarabilities of the competency See Repairs S | Competency 3e: Modifies network infrastructure to serve new purposes or improve workflow | | Advanced | Operate and Maintain | Network Services | |
| seaske parties Competency II. Regime network connectivity problems Competency II. Fest and maintains network infrastructure including software and hardware devices. Competency II. Fest and maintains network infrastructure including software and hardware devices. Competency II. Fest and maintains network infrastructure including software and hardware devices. Competency II. Implements occurring measures for turns in system and entures that system. Competency II. Implements occurring measures for turns in system and entures that system. Competency II. Implements occurring measures for turns in system and entures that system. Competency II. Implements occurring measures for turns in system and entures that system. Competency III. Implements occurring measures for turns in system and entures that shows a system and entures that system and entures that system and entures that system and entures that shows a system and enture that shows a system and entures | | | Intermediate | Operate and Maintain | Network Services | |
| Source Opposition 51. Section of maintains received infinitionation mediating software and fundamend decreases. Composition 51. Section of maintains sections of intermediate of provinge and Composition 52. Section of Maintains and Composition 52. Section of Maintains Associated Section 52. Se | | | Intermediate | Operate and Maintain | Network Services | |
| Basic Operate Minimals recover combis based on principles of least privilege and seed to above the competency \$1. Employees possible and control to above the competency \$2. Employees \$2 | Competency 3h: Repairs network connectivity problems | | Basic | Operate and Maintain | Network Services | |
| Competency - 1) Establishes adequate access controls based on principles of Seat privilege and Competency - 1) Establishes adequate access controls between the confidentiality, situating response to the confidentiality, situating value and substitution of the confidentiality, situating value and value of the confidentiality, situating situations and confidentiality, situating value of the confidentiality and confidentiality, situating value of the confidentiality and confidentiality, situati | Competency 3i: Tests and maintains network infrastructure including software and hardware device | es | Basic | Operate and Maintain | Network Services | |
| Competency & Conducts procedure or security recurrence for users in system and essues that you will be a security of the state of the s | Competency 3j: Establishes adequate access controls based on principles of least privilege and need-to-know | | | | Systems Security | |
| earmer before confidentially, integring and availability, alter manages accounts, frevails or configuration, make advantability management. It responsible for success control, security configuration and administration and monotoning data doministration and monotoning data | | | Basic | | | |
| Competency 4r. Conducts functional and connectivity testings to ensure continuing operability Competency 4r. Conducts periodic server maintenance including cleaming physically and electronically, disk checks, yester configuration and monitoring, dust downloads, bedueps and setting and electronically, disk checks, yester configuration and monitoring, dust downloads, bedueps and setting and electronically, disk checks, yester configuration and monitoring, dust downloads, bedueps and setting and electronically, disk checks, yester configuration and monitoring, dust downloads, bedueps and setting and electronically, disk checks, yesters and electronically and the properties and electronically and the competency of the properties and electronically and the properties and electronically and the properties of the properties proceedings. Competency 4r. Description of the properties and electronically and electronic and electroni | ensure their confidentiality, integrity and availability; also manages accounts, firewalls, configuration, patch and vulnerability management. Is responsible for access control, security configuration and administration | | | | | |
| Competency 4c: Combots periodic server maintenance including clearing (physically and electronically), disk checks, system configuration and monitoring, data downloads, backups and electronically), disk checks, system configuration and monitoring, data downloads, backups and electronically), disk checks, system configuration and monitoring, data downloads, backups and electronically), disk checks, system configuration and monitoring data downloads, backups and electronically), disk checks, system definition and monitoring and encods Competency 4d: Nations in the development of group policies and access control lists to ensure computational programment of the programmen | | | Intermediate | Operate and Maintain | System Admin | |
| Basic Operate and Maintain System Admin Competency 4E. Nassis in the development of group policies and access control lists to ensure computatively with organizational standard, business rules and needs. Competency 4E. Documents compliance with or changes to system administration standard operate and Maintain System Admin Intermediate Operate and Maintain System Admin Competency 4E. Documents compliance with or changes to system administration standard operating procedures. Competency 4E. Installs server fixes, updates and enhancements Competency 4E. Installs server fixes, updates and enhancements Competency 4E. Maintains Standard systems security according to organizational policies Competency 4E. Maintains Standard systems security according to organizational policies Competency 4E. Maintains Standard systems and equipment Competency 4E. Maintains server configuration Competency 4E. Verifies data redundancy and system recovery procedures Competency 4E. National Competency 4E. Maintains server competency and maintains or restrict and maintains or restrict and problems on the configuration or installation of new or modified hardware, operating systems and other hardware server restrict and problems of the server restrict and interoperability problems Competency 4E. Relabilities adaptate access controls based on principles of least privilege, role Competency 5E. Configures tools and technologies to det | | | Basic | Operate and Maintain | System Admin | |
| Competency Aff. Actiss: in the development of group policies and access control lists to ensure compatibility with organizational standards, business rules and looks. Advanced Operate and Maintain System Admin System Admin policies of the Competency Aff. Maintains baseline system security according to organizational policies Competency Aff. Maintains baseline system security according to organizational policies Competency Aff. Maintains baseline system security according to organizational policies Competency Aff. Maintains baseline system security according to organizational policies Competency Aff. Maintains baseline system security according to organizational policies Competency Aff. Maintains baseline system security according to organizational policies Competency Aff. Maintains baseline system security according to organizational policies Competency Aff. Maintains baseline system security according to organizational policies Competency Aff. Maintains baseline system administration and problems of the system administration and maintains server configuration Competency Aff. Maintains baseline system administration and problems of the system administration and maintains server configuration Competency Aff. Monitors and maintains server configuration Competency Aff. Monitors and maintains server configuration Competency Aff. Verifies data redundancy and system recovery procedures Competency Aff. Verifies data redundancy and system recovery procedures Competency Aff. Provides undown software and interpretability problems of the competency aff. Provides undown software and interpretability problems of the competency of the Provides undown software and interpretability problems. Competency Aff. Provides undown software interface and interpretability problems of the system administration of security patches for committee and interpretability problems. Competency Sc. Maintain Colora and Defend Defend Defend Defend Defend Defend Competency Sc. Maintains Colora and Defend Defend Defend Defend Advanced | electronically), disk checks, system configuration and monitoring, data downloads, backups and | | | | | |
| Competency 4: Documents compliance with or changes to system administration standard operating procedures Competency 4: Documents compliance with or changes to system administration standard operating procedures Competency 4: Installs server fixes, updates and enhancements Competency 4: Maintains baseline system security according to organizational policies Competency 4: Manages accounts, network rights and access to systems and equipment Competency 4: Monitors and maintains server configuration Competency 4: Supports network, components Competency 4: Supports network components Competency 4: Supports network components Competency 4: Verifies data redundancy and system recovery procedures Competency 4: Verifies data redundancy and system recovery procedures Competency 4: Verifies data redundancy and system recovery procedures Competency 4: Provides data redundancy and system recovery procedures Competency 4: Provides ongoing optimization of new or modified hardware, operating systems and other baselines software Competency 4: Recovers and water servers and the continuation or installation of new or modified hardware, operating systems and other baselines software Competency 4: Recovers hardware/software interface and interoperability problems Competency 4: Recovers hardware/software interface and interoperability problems Competency 4: Recovers hardware/software interface and interoperability problems Competency 5: Configurate tools and technologies to detect, mitigate and prevent potential devents of the continuation of the problems of the continuation of the contin | Competency 4d: Assists in the development of group policies and access control lists to ensure | | Basic | Operate and Maintain | System Admin | |
| Competency 4f. Initially server fixes, updates and enhancements Competency 4g. Maintains baseline system security according to organizational policies Intermediate Operate and Maintain System Admin Competency 4f. Manages accounts, network rights and access to systems and equipment Competency 4f. Monitors and maintains server configuration Competency 4f. Monitors and maintains server configuration Competency 4f. Monitors and maintains server configuration Competency 4f. Supports network components Competency 4f. Verified data reclundancy and system recovery procedures Competency 4f. Verified data reclundancy and system recovery procedures Competency 4ff. Verified data reclundancy and system recovery procedures Competency 4ff. Verified data reclundancy and system recovery procedures Competency 4ff. Verified data reclundancy and system recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 4ff. Verified data reclundancy and postem recovery procedures Competency 5ff. Conditions with recover administrators to administer the updating of rules and verified to postem recovery procedures and postem recovery procedures and postem recovery procedures Competency 5ff. Ensures | , | | Advanced | Operate and Maintain | System Admin | |
| Competency 4g: Maintains baseline system security according to organizational policies Intermediate Operate and Maintain System Admin Competency 4i: Monitors and maintains server configuration Intermediate Operate and Maintain System Admin Competency 4i: Monitors and maintains server configuration Intermediate Operate and Maintain System Admin Competency 4i: Supports network components Competency 4i: Verified data redundancy and system recovery procedures Competency 4i: Verified data redundancy and system recovery procedures Competency 4ii: Provides organize government control of the confination or installation of new or modified hardware, operating systems and often buseline software interface and interoperability problems Competency 4ii: Provides organize government and deep buseline software interface and interoperability problems Competency 4ii: Provides organize government and deep software interface and interoperability problems Basic Operate and Maintain System Admin Competency 4ii: Provides organize government and deep software interface and interoperability problems Basic Operate and Maintain System Admin Competency 4ii: Provides organize government and deep software interface and interoperability problems Basic Operate and Maintain System Admin Competency 5ii: Configures tools and technologies to detect, mitigate and prevent potential threats Competency 5ii: Configures tools and technologies to detect, mitigate and prevent potential threats Competency 5ii: Natalla and maintains cyber security detection, monitoring and threat managements officially and security detection, monitoring and analysis of system activity to detect on systems, and network black and white list competency 5ii: Natalla and maintains and network definit | operating procedures | | Intermediate | Operate and Maintain | System Admin | |
| Competency 4ir. Manages accounts, network rights and access to systems and equipment Competency 4ir. Monitors and maintains server configuration Competency 4ir. Supports network components Competency 4ir. Supports network components Competency 4ir. Supports flavore hardware; seeks appropriate support or assistance to perform server repairs Competency 4ir. Verifies data redundancy and system recovery procedures Competency 4ir. Verifies data redundancy and system recovery procedures Competency 4ir. Verifies data redundancy and system recovery procedures Competency 4ir. Verifies data redundancy and system recovery procedures Competency 4ir. Verifies data redundancy and system recovery procedures Competency 4ir. Verifies data redundancy and system recovery procedures Competency 4ir. Provides ongoing optimization or installation of new or modified hardware, operating systems and other baseline software Competency 4ir. Provides ongoing optimization and problem-solving support Competency 4ir. Provides ongoing optimization of install support installation of inst | Competency 4g: Maintains baseline system security according to organizational policies | | Intermediate | Operate and Maintain | System Admin | |
| Competency 4: Monitors and maintains server configuration Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Competency 4: Diagnoses faulty system/server pairs Competency 4: Diagnoses faulty system/server pairs Competency 5: Diagnoses faulty system/server pairs Competency 5: Installs and maintain system daminis System Admin System System Syste | Competency 4h: Manages accounts, network rights and access to systems and equipment | | Intermediate | Operate and Maintain | System Admin | |
| Competency 4: Supports network components Competency 4: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs Basic Operate and Maintain System Admin Competency 4: Verifies data redundancy and system recovery procedures Competency 4: Verifies data redundancy and system recovery procedures Intermediate Operate and Maintain System Admin Competency 4n: Provides ongoing optimization or installation of new or modified hardware, operating systems and other baseline admirate and interoperability problems Competency 4n: Provides ongoing optimization and problem-solving support Intermediate Operate and Maintain System Admin Operate and Maintain System Security Operat | Competency 4i: Monitors and maintains server configuration | | | | | |
| Sassiance to perform server repairs Competency 41: Verifies data redundancy and system recovery procedures Intermediate Competency 42: Verifies data redundancy and system recovery procedures Intermediate Competency 43: Sassis in the coordination or installation of new or modified hardware, operating systems and other baseline software Competency 44: Nesists in the coordination or installation of new or modified hardware, operating systems and other baseline software Competency 44: Provides ongoing optimization and problem-solving support Competency 45: Resolves hardware/software interface and interoperability problems Competency 46: Establishes adequate access controls based on principles of least privilege, role based access controls (RBAC) and need-to-know Competency 55: Configures tools and technologies to detect, mitigate and prevent potential threats Competency 55: Configures tools and technologies to detect, mitigate and prevent potential threats Competency 56: Coordinates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus and network black and white list Competency 56: Manages IP addresses based on current threat environment Competency 56: Ensures application of security patches for commercial products integrated into system design Competency 56: Uses computer network defense tools for continual monitoring and analysis of systems activity to identify malicious activity Advanced Protect and Defend Compater Network Defense Analysis Competency 56: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Intermediate Operate and Maintain System Admin System Security Advanced Operate and Maintain Competency 61: Ensures application of security patches for commercial products | | | | | , | |
| Competency 4: Verifies data redundancy and system recovery procedures Intermediate Operate and Maintain System Admin Competency 4: Provides ongoing optimization and problem-solving support Competency 4: Provides ongoing optimization and interface and interoperability problems Basic Operate and Maintain System Admin Sys | Competency 4k: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs | | Basic | Operate and Maintain | System Admin | |
| Operating systems and other baseline software Competency 4n: Provides ongoing optimization and problem-solving support Intermediate Operate and Maintain Operate and Maintain System Admin Operate and Maintain Operate and Maintain Operate and Maintain System Admin Operate and Maintain Operate and Maintai | Competency 4l: Verifies data redundancy and system recovery procedures | | Intermediate | Operate and Maintain | System Admin | |
| Competency 4n: Provides ongoing optimization and problem-solving support Competency 4o: Resolves hardware/software interface and interoperability problems Basic Operate and Maintain System Admin Operate and Maintain System Security Advanced Operate and Maintain Operate and Maintain System Security Advanced Operate and Maintain Operate and Maintain System Security Advanced Operate and Maintain Operate and Maintain System Security Analysis Operate and Maintain Operate and Maintain System Security Analysis Operate and Maintain Op | | | Intermediate | Operate and Maintain | System Admin | |
| Competency 4o: Resolves hardware/software interface and interoperability problems Competency 4p: Establishes adequate access controls based on principles of least privilege, role based access controls (RBAC) and need-to-know Advanced Operate and Maintain JOB FUNCTION 5: Configures tools and technologies to detect, mitigate and prevent potential threats Competency 5a: Installs and maintains cyber security detection, monitoring and threat management software Competency 5b: Coordinates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus and network black and white list Competency 5c: Manages IP addresses based on current threat environment Competency 5d: Ensures application of security patches for commercial products integrated into system design Competency 5c: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity JOB FUNCTION 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities Competency 6a: Applies security policies to meet security objectives of the system Competency 6b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6c: Insures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6c: Insures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6c: Insures that data back up and restoration of any computer network defense tools. Performs tool signature testing and optimization Competency 6c: Insures that data back up and applications are functional and consistent with company's document retention policy and business continuity needs Competency 6c: Insures that data back up and optimization Competency | Competency 4n: Provides ongoing optimization and problem-solving support | | | | | |
| Competency 4p: Establishes adequate access controls based on principles of least privilege, role based access controls (RBAC) and need-to-know and seed access controls (RBAC) and need-to-know and personal products integrated into signatures for intrusion/detection protection systems, anti-virus and network black and white list competency 5e: Conditates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus and network black and white list competency 5e: Manages IP addresses based on current threat environment lintermediate Competency 5e: Insures application of security patches for commercial products integrated into system design Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Competency 6e: Advanced Protect and Defend Systems security analysis Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Competency 6e: Advanced Protect and Defend Systems security analysis Competency 6e: Applies security policies to meet security objectives of the system Intermediate Operate and Maintain Systems Security Analysis Systems Security Analysis Systems Security Analysis Competency 6e: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6e: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6e: Identifies potential conflicts with implementation of any computer network defense tools lig | Competency 4o: Resolves hardware/software interface and interoperability problems | | | | | |
| JOB FUNCTION 5: Configures tools and technologies to detect, mitigate and prevent potential threats Competency 5a: Installs and maintains cyber security detection, monitoring and threat management software Competency 5b: Coordinates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus and network black and white list Competency 5c: Manages IP addresses based on current threat environment Competency 5d: Ensures application of security patches for commercial products integrated into system design Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Advanced Protect and Defend Systems security analysis Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Advanced Protect and Defend Systems security analysis Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Advanced Protect and Defend Systems security analysis Competency 6e: Applies security policies to meet security objectives of the system Intermediate Operate and Maintain Operate and Maintain Operate and Maintain Operate and Maintain Analysis Systems Security Analysis | | | | | Systems Security | |
| Competency 5a: Installs and maintains cyber security detection, monitoring and threat management software Competency 5b: Coordinates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus and network black and white list Competency 5c: Manages IP addresses based on current threat environment Competency 5d: Ensures application of security patches for commercial products integrated into system design Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Advanced Protect and Defend Computer Network Defense Analysis Operate and Maintain Systems security analysis Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Intermediate Operate and Maintain Systems Security Advanced Protect and Defend Computer Network Defense Analysis Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Intermediate Operate and Maintain Operate and Maintain Systems Security Analysis Competency 6b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6c: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6c: Identifies potential conflicts with implementation of any computer network defense tools, Performs tool signature testing and optimization | | | Advanced | Operate and Maintain | Analysis | |
| Competency 5b: Coordinates with network administrators to administer the updating of rules and signatures for intrusion/detection protection systems, anti-virus and network black and white list Competency 5c: Manages IP addresses based on current threat environment Intermediate Competency 5d: Ensures application of security patches for commercial products integrated into system design Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Advanced Protect and Defend Systems security analysis Systems security analysis Operate and Maintain From the twork before a Analysis Systems security analysis Intermediate Operate and Maintain Operate and Maintain Systems Security Analysis Competency 6a: Applies security policies to meet security objectives of the system Competency 6b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6c: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization | Competency 5a: Installs and maintains cyber security detection, monitoring and threat | | Intermediate | Duotant and Dafond | Computer Network | |
| Competency 5c: Manages IP addresses based on current threat environment Competency 5d: Ensures application of security patches for commercial products integrated into system design Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity JOB FUNCTION 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities Competency 6a: Applies security policies to meet security objectives of the system Competency 6b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6c: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization | | | | | Computer Network | |
| Competency 5d: Ensures application of security patches for commercial products integrated into system design Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity Advanced Protect and Defend Advanced Protect and Defend Systems security analysis Computer Network Defense Analysis Intermediate Competency 6a: Applies security policies to meet security objectives of the system Competency 6b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6c: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization | | | | Frotest and Defend | Defense Analysis | |
| Competency 5e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity JOB FUNCTION 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities Competency 6a: Applies security policies to meet security objectives of the system Competency 6b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6c: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization | | | | Operate and Maintain | | |
| JOB FUNCTION 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities Competency 6a: Applies security policies to meet security objectives of the system Competency 6b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6c: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization Systems Security Analysis Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization | | | | | Computer Network | |
| Intermediate Operate and Maintain Systems Security Analysis Competency 6b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6c: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6c: Insures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6c: Insures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6c: Insures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6c: Insures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Systems Security Analysis Competency 6c: Insures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Systems Security Analysis | | | Auvanced | Froiect and Defend | Detense Analysis | |
| Competency 6b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices Competency 6c: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization Systems Security Analysis Systems Security Analysis Systems Security Systems Security Systems Security Analysis | Competency 6a: Applies security policies to meet security objectives of the system | | Intermediate | Operate and Maintain | | |
| Competency 6c: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization Systems Security Analysis Systems Security Systems Security | | | | | Systems Security | |
| Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization Systems Security | Competency 6c: Ensures that data back up and restoration systems are functional and consistent | | | | Systems Security | |
| | | | | | Systems Security | |

| Competency 6e: Installs, manages and updates intrusion detection system | | | | |
|--|-------------------|---|---|--|
| competency oc. Instants, manages and apparets mutason detection system | Advanced | Operate and Maintain | Systems Security Analysis | |
| Competency 6f: Performs technical and non-technical risk and vulnerability assessments of relevant technology focus areas | Advanced | Protect and Defend | Vulnerability Assessment and | |
| Competency 6g: Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results | Intermediate | Protect and Defend | Management Vulnerability Assessment and | |
| Competency 6h: Documents systems security operations and maintenance activities | | | Management Systems Security | |
| Competency6i: Communicates potential risks or vulnerabilities to manager. Collaborates with others to recommend vulnerability corrections | Advanced Advanced | Operate and Maintain Protect and Defent | Computer Network Defense and Analysis | |
| Competency6j: Identifies information technology security program implications of new technologies or technology upgrades | Advanced | Protect and Defend | Computer Network Defense and Analysis | |
| JOB FUNCTION 7: Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats | | | | |
| Competency 7a: Identifies organizational trends with regard to the security posture of systems; identifies unusual patterns or activities | | | Systems Security | |
| Competency 7b: Characterizes and analyzes network traffic to identify anomalous activity and potential threats; performs computer network defense trend analysis and reporting | Basic | Operate and Maintain | Analysis Computer network | |
| Competency 7c: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | Advanced | Protect and Defend | Defense and Analysis Computer network | |
| Competency 7d: Runs tests to detect real or potential threats, viruses, malware, etc. | Advanced | Protect and Defend | Defense and Analysis | |
| Competency 7e: Assists in researching cost-effective security controls to mitigate risks | Advanced | | Vulnerability | |
| Competency 7f: Helps perform damage assessments in the event of an attack | Intermediate | Protect and Defend | Assessment and | |
| | Advanced | | | |
| Competency 7g Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities | Advanced | Operate and Maintain | Systems Security Analysis | |
| Competency 7h: Documents and escalates incidents that may cause immediate or long-term impact to the environment | Intermediate | Protect and Defend | Computer network Defense Analysis | |
| Competency 7i: Provides timely detection, identification and alerts of possible attacks and intrusions, anomalous activities, and distinguish these incidents and events from normal baseline activities | A J | Donate of and Dofeed | Computer network | |
| Competency 7j: Uses network monitoring tools to capture and analyze network traffic associated with malicious activity | Advanced | Protect and Defend | Defense Analysis | |
| Competency 7k: Performs intrusion analysis | Advanced | Investigate | Digital Forensics | |
| Competency 71: Sets containment blockers to align with company policy regarding computer use and web access | Intermediate | Investigate Protect and Defend | Digital Forensics Computer network Defense Analysis | |
| JOB FUNCTION 8: Responds to cyber intrusions and attacks and provides defensive strategies | | | | |
| Competency 8a: Assists in the development of appropriate courses of action in response to | | | | |
| identified anomalous network activity | Advanced | Protect and Defend | Computer network Defense Analysis | |
| Competency 8b: Triages systems operations impact: malware, worms, man-in-the-middle attack, denial of service, rootkits, keystroke loggers, SQL injection and cross-site scripting | Advanced | Protect and Defend | Computer network Defense Analysis | |
| Competency 8c: Reconstructs a malicious attack or activity based on network traffic | Advanced | Protect and Defend | Computer network Defense Analysis | |
| Competency 8d: Correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation | Advanced | Protect and Defend | Incident Response | |
| Competency 8e: Monitors external data sources to maintain currency of Computer Network Defense threat condition and determines which security issues may have an impact on the enterprise. Performs file signature analysis | Advanced | Protect and Defend | Incident Response | |
| Competency 8f: Performs analysis of log files from a variety of sources to identify threats to network security; performs file signature analysis | Advanced | Protect and Defend | Incident Response | |
| Competency 8g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | Advanced | Protect and Defend | Incident Response | |
| Competency 8h: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | Advanced | Protect and Defend | Incident Response | |
| Competency 8i: Tracks and documents computer network defense incidents from initial detection through final resolution | Intermediate | Protect and Defend | Incident Response | |
| Competency 8j: Collects intrusion artifacts and uses discovered data to enable mitigation of potential computer network defense (CND) incidents | Advanced | Protect and Defend | Incident Personal | |
| Competency 8k: Performs virus scanning on digital media | Advanced Basic | Protect and Defend Investigate | Incident Response Digital forensics | |
| | | | | |

| RELATED INSTRUCTION | NICE Framework | Core/Optional | LEVEL |
|--|----------------|---------------|--------|
| o | | | |
| Skills | | | |
| Conducting research to identify new threats and threat mitigation strategies | T0503 | | |
| Following trade publications to stay current on threats and threat mitigation techniques | T0503 | | |
| Gauging learner understanding levels | S0066/S0070 | | |
| Interfacing with customers | S0011 | | |
| Applying confidentiality, integrity and availability principles Knowledge & Understanding | S0006 | | |
| Computer networking concepts and protocols and network security methodology | K0001 | | |
| Methods for assessing and mitigating risk | K0002 | | |
| National and international laws, regulations, policies and ethics as they relate to cybersecurity | K0003 | | |
| Cybersecurity principles | K0004 | | |
| Cyber threats and vulnerabilities | K0005 K0006 | | |
| Specific operational impacts of cybersecurity lapses Authentication, authorization and access control methods | K0006 | | |
| Known vulnerabilities from alerts, advisories, errata and bulletins | K0040 | | |
| Cybersecurity principles and organizational requirements relevant to confidentiality, integrity, availability, authentication and non-repudiation | K0040 | | |
| Enterprise's IT goals and objectives | K0101 | | |
| Organization's core business/mission processes | K0146 | | |
| * | K0146 K0158 | | |
| Organizational IT use security policies (e.g. account creation, password rules, access control) | | | |
| Personally identifiable information data security standards | K0260 | | |
| Payment card industry data security standards | K0261 | optional | |
| Personal health information data security standards | K0262 | optional | |
| Operations and processes for incident, problem, and event management | K0292 | | |
| Risk Management Framework Requirements | K0048 | | |
| Cloud-based knowledge management technologies and concepts related to security, governance, | K0194 | | |
| procurement and administration Organizational traning policies | K0215 | | |
| Tools & Technologies | K0213 | | |
| 1003 & Technologies | | | |
| Intranet | | | |
| Electronic mail | | | |
| Word processing software | | | |
| Electronic search and reference platforms | | | |
| Remote access technologies | | | |
| Desktop computers, laptop computers, tablets, smartphones and other personal IT devices ETENCIES | | | |
| Competency a: Locates (in intranet, employee handbook or within software) organizational policies | T0461 | Core | Basic |
| intended to maintain security and minimize risk and explains their use | | | |
| Performance Standards | | | |
| Identifies location of company or organization's IT security policies Identifies policies aligned with each IT system, potential sources of vulnarability and general security principles | | | |
| Explains to others the vulnerabilities and risks associated with policy violations | | | |
| Compares current policies with recommended policies to ensure alignment with current threats | | | |
| Identifies gaps between current policies and contemporary threats | | | |
| Recommends new policies or modifications to old policies to align with current threats | | | |
| | | | |
| Competency b: Provides guidance to employees on how to access networks, set passwords, reduce | T0192 | Optional | Advanc |
| security threats and provide defensive measures associated with searches, software downloads, email, Internet, add-ons, software coding and transferred files | 10172 | Optional | Auvano |
| 2. 1. 1 | | | |
| Performance Standards | | | |

| Competency c: Ensures that password characteristics are explained and enforced and that updates are required and enforced based on appropriate time intervals | | Core | Basic |
|---|-------------|----------|------------|
| Performance Standards | | | |
| Identifies organization's policies regarding passwords and compares it will current recommendations Explains to employees how to establish a password that meets the company's security requirements | | | |
| | | | |
| Establishes intervals for requiring employees to change their passwords Notifies employees when a new password is required | | | |
| Notifies employees when a new password is required | | | |
| | | | |
| | | | |
| | | | |
| | | | - |
| Competency d: Explains company or organization's policies regarding the storage, use and transfer of sensitive data, including intellectual property and personally identifiable information. Identifies data life cycle, data storage facilities, technologies and describes business continuity risks | T0458/T0871 | Core | Intermedia |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | TO 161 TO 2 | | |
| Competency e: Assigns individuals to the appropriate permission or access level to control access to certain web IP addresses, information and the ability to download programs and transfer data to various locations | T0461/T0054 | Optional | Advanced |
| Performance Standards | | 1 | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency f: Assists employees in the use of technologies that restrict or allow for remote access to the organization's information technology network | T0144 | Core | Intermedia |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency g: Develops security compliance policies and protocols for external services (i.e. Cloud service providers, software services, external data centers) | T0136 | Optional | Advanced |
| | | | |
| Performance Standards | | | |
| | T0331 | Optional | Advanced |
| Competency h: Complies with incident response and handling methodologies | T0331 | Optional | Advanced |
| | T0331 | Optional | Advanced |
| Competency h: Complies with incident response and handling methodologies | T0331 | Optional | Advanced |
| Competency h: Complies with incident response and handling methodologies | T0331 | Optional | Advanced |
| Competency h: Complies with incident response and handling methodologies | T0331 | Optional | Advanced |

| Competency i: Articulates the business need or mission of the organization as it pertains to the use of IT systems and the storage of sensitive data | K0416 | Core | Intermedia |
|--|-------|------|------------|
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| RELATED INSTRUCTION | NICE Framework | Core/Optional | LEVEL |
|---|------------------|---------------|---------|
| Skills | TVICE Trainework | Core/Optional | LLVLL |
| Skills | | | |
| Conducting research for client-level problems | S0142 | | |
| Identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degredation | S0039 | | |
| Using appropriate tools for repairing software hardware and peripheral equipment of a system | S0058 | | |
| Operating system administration | S0158 | | |
| Installing system and component upgrades | S0154 | | |
| Configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications | S0159 | | |
| Knowledge & Understanding - Italicized knowledge standards are repeated from an earlier job function | | | |
| | | | |
| K0001 - K0006 from job function 1 | K0001-6 | | |
| Measures or indicators of system performance | K0053 K0088 | | |
| System administration concepts Industry best practices for service desk | K0088 K0237 | | |
| Organizational security policies | K0237 | | |
| Remote access processes, tools and capabilities related to customer support | K0247 | | |
| Personal and sensitive data security standards | K0247 | | |
| • | | | |
| Information technology risk management policies, requirements and procedures | K0263 | | |
| The organization's information classification program and procedures for information compromise | K0287 | | |
| Operations and processes for incident, problem and event management | K0292 | | |
| IT system operation, maintenance and security needed to keep equipment functioning properly | K0294 | | |
| Basic operation of computers | K0302 | | |
| Procedures for document and querying reported incidents, problems and events | K0317 | | |
| Organization's evaluation and validation criteria | K0330 | | |
| Tools & Technologies | | | |
| Electronic devices e.g. (computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems | K0114 | | |
| Common network tools (e.g. ping, traceroute, nslookup) | K0306 | | |
| | | | |
| | | | |
| | | | |
| ETENCIES | | | |
| Competency a: Manages inventory of IT resources | T0496 | Core | Basic |
| Performance Standards | | | |
| · ···································· | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency b: Diagnoses and resolves customer-reported system incidents | T0482 | Core | Interme |
| | | | |
| Performance Standards | | | |

| Competency c: Installs and configures hardware, software and peripheral equipment for system users | T0491 | Core | Basic |
|--|--------------------------|------|-------------|
| Performance Standards | | | |
| renormance standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency d: Monitors client-level computer system performance | T0468 | Core | Basic |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency e: Tests computer system performance | T0502 | Core | Basic |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency f: Troubleshoots system hardware and software | T0237 | Core | Basic |
| Performance Standards | 10237 | Corc | Basic |
| 1 enormance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency g: Administers accounts, network rights, and access to systems and equipment | T0494/TO144 | Core | Intermedia |
| Competency g: Administers accounts, network rights, and access to systems and equipment Performance Standards | T0494/T0144 | Core | Intermedia |
| | T0494/T0144 | Core | Intermedia |
| Performance Standards Competency h: Implements security measures for uses in system and ensures that system designs | T0494/T0144 T0136/T0485 | Core | Intermedia |
| Performance Standards Competency h: Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines | | | |
| Performance Standards Competency h: Implements security measures for uses in system and ensures that system designs | | | |
| Performance Standards Competency h: Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines | | | |
| Performance Standards Competency h: Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines | | | Intermediat |

| RELATED INSTRUCTION | NICE Framework | Core/Optional | LEVEL |
|---|----------------|---------------|-------|
| Skills | | | |
| | Good | | |
| Analyzing network traffic capacity and performance characteristics Establishing a routing scheme | S0004 S0035 | | |
| Implementing, maintaining and improving established network security practices | S0040 | | |
| installing, configuring and troubleshooting LAN and WAN components such as routers, hubs and switches | | | |
| Using network management tools to analyze network traffic patterns (e.g. simple network management protocol) | S0056 | | |
| Securing network communications | S0077 | | |
| Protecting a network against malware | S0079 | | |
| Configuring and utilizing network protection components (e.g. firewalls, VPNs, network intrusion detection systems) | S0084 | | |
| Implementing and testing network infrastruture contingency and recovery plans | S0150 | | |
| Applying cybersecurity methods, such as firewalls, demilitarized zones and encryption | S0168 | | |
| Digital rights management | | | |
| Operating network equipment including hubs, routers, switches, bridges, servers, transmission media and related hardware | A0052 | | |
| Executing OS command line (e.g. ipconfig, netwtat, dir, nbstat) | A058 | | |
| Knowledge & Understanding | | | |
| See K0001 through K0006 from job function 1 | K001-6 | | |
| Communication methods, principles and concepts (e.g. crypto, dual hubs, time multiplexers) that support the network infrastructure | K0010 | | |
| Capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, ransmission media and related hardware | K0011 | | |
| Organization's LAN/WAN pathways | K0029 | | |
| Cybersecurity principles used to manage risks related to the use, process, storage and transmission of information or data | K0038 | | |
| T security principles and methods including firewalls, encryption, etc. | K0049 | | |
| Local area and wide area networking principles and concepts including bandwidth management | K0050 | | |
| Measures or indicators of system performance and availability Fraffic flow across the network (e.g. transmission control protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [TTIL]) | K0053 K0061 | | |
| Remote access technology concepts | K0071 | | |
| T supply chain security and risk mangement policies, requirements and procedures | K0169 | | |
| Network security architecture concepts including topology, protocols, components and principles | K0179 | | |
| Windows/Unix ports and services | K0192 | | |
| Telecommunication concepts (e.g. routing algorithms, fiber optics systems link budgeting, add/drop multiplexers) | K0093 | | |
| Virtual private network security principles | K0104 | | |
| Concepts, terminology and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless) | K0108 | | |
| Different types of network communication (LAN/WAN/WAN/WLAN/WWAN) | K0113 | | |
| Web filtering technologies | K0135 | | |
| Capabilities of different electronic communication systems and methods (email, VOIP, IM, web forums, Direct Video Broadcasts, etc.) | K0136 K0159 | | |
| Range of existing networks (PBX, LANs, WANs, WIFI, SCADA) | K0137 | | |
| Principles and operation of Wi-Fi | K0138 | | |
| Network systems management principles, models, methods (e.g. end-to-end systems performance monitoring) and tools | K0181 | | |
| Fransmission records (e.g. Bluetooth, Radio Frequency Identification, Infrared Networking, Wireless Fidelity, paging, cellular, satellite dishes) and jamming techniques that enable transmission of undesirable | K0181 | | |

| Service management concepts for networks and related standards (e.g. ITIL) | K0200 | | |
|---|-------------|----------|----------|
| Common networking protocols, services and how they interact to provide network communications | K0099 | | |
| Common network tools (e.g. ping, tracerouite, nslookup) | K0307 | | |
| Local area network, wide area network and enterprise principles and concepts, including bandwidth | K0327 | | |
| management Network protocols (TCP, IP, DHCP and directory services, e.g. DNS) | K0331 | | |
| | | | |
| Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System and directory services | K0332 | | |
| Principles and methods for integrating system components | K0346 | | |
| Tools & Technologies | | | |
| Network tools | | | |
| Hubs, switches, routers, bridges, servers, transmission media | | | |
| Electronic communication systems Bluetooth, RFID, IR, Wi-Fi, paging, cellular and satellite dishes | | | |
| Buetouli, Krid, ik, wi-ri, paging, centual and sateline dishes | | | |
| IPETENCIES | | | |
| Competency a: Collaborates with system developers and users to assist in the selection of appropriate | T0200/T0201 | Optional | Advanced |
| design solutions to ensure the compatibility of system components | 10200/10201 | Ориона | Advanced |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency b: Installs, replaces, configures and optimizes network hubs, routers and switches | T0035/T0126 | Optional | Advanced |
| D. C Ct I I. | | | |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | TOM | | |
| Competency c: Assists in network backup and recovery procedures | T0065 | Optional | Advanced |
| Competency c: Assists in network backup and recovery procedures Performance Standards | T0065 | Optional | Advanced |
| 1 | T0065 | Optional | Advanced |
| 1 | T0065 | Optional | Advanced |
| 1 | T0065 | Optional | Advanced |
| 1 | T0065 | Optional | Advanced |
| 1 | T0065 | Optional | Advanced |
| 1 | T0065 | Optional | Advanced |
| Performance Standards | T0065 | | Advanced |
| Performance Standards Competency d: Diagnoses network connectivity problems | | Optional | |
| Performance Standards | | | |
| Performance Standards Competency d: Diagnoses network connectivity problems | | | |
| Performance Standards Competency d: Diagnoses network connectivity problems | | | |
| Performance Standards Competency d: Diagnoses network connectivity problems | | | |
| Performance Standards Competency d: Diagnoses network connectivity problems | | | |
| Performance Standards Competency d: Diagnoses network connectivity problems | | | |
| Performance Standards Competency d: Diagnoses network connectivity problems | | | |
| Performance Standards Competency d: Diagnoses network connectivity problems | | | |

| Performance Standards | | | | <u> </u> |
|---|--|-------------|----------|--------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Competency f: Integrates new systems into existing | ng network architecture | T0121/T0129 | Optional | Advanced |
| | | | ~ p | |
| Performance Standards | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Competency g: Patches network vulnerabilities to | ensure information is safeguarded against outside | T0125/T0160 | Optional | Advanced |
| parties | | | | |
| Performance Standards | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Competency h: Repairs network connectivity prob | olems | T0081 | Optional | Advanced |
| Performance Standards | | | | |
| Performance Standards | | <u> </u> | 1 | ı |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Comparance is Tosts and maintains natural info | otwotwo including software and bardware devices | T0152/T0222 | Coro | Intermediate |
| Competency i: Tests and maintains network infras | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| Competency i: Tests and maintains network infras | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| Performance Standards | | | | |
| Performance Standards Competency j: Establishes adequate access contro | structure including software and hardware devices | T0153/T0232 | Core | Intermediat |
| Performance Standards | | | | |
| Performance Standards Competency j: Establishes adequate access contro | | | | |
| Performance Standards Competency j: Establishes adequate access controknow | | | | |
| Performance Standards Competency j: Establishes adequate access controknow | | | | |
| Performance Standards Competency j: Establishes adequate access controknow | | | | |
| Performance Standards Competency j: Establishes adequate access controknow | | | | |
| Performance Standards Competency j: Establishes adequate access controknow | | | | |
| Performance Standards Competency j: Establishes adequate access contro know | | | | |
| Performance Standards Competency j: Establishes adequate access contro know | | | | |
| Performance Standards Competency j: Establishes adequate access controknow | | | | |
| Performance Standards Competency j: Establishes adequate access controknow | | | | |
| Performance Standards Competency j: Establishes adequate access contro know Performance Standards | ls based on principles of least privilege and need-to- | T0475 | Core | |
| Performance Standards Competency j: Establishes adequate access controknow | ls based on principles of least privilege and need-to- | | | |

| Performance Standards | | |
|-----------------------|--|--|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| RELATED INSTRUCTION | NICE | Core/Optional | LEVEL |
|---|----------------|---------------|-------|
| | Framework | • | |
| Skills | | | |
| 5. 8. 5. F. 8 F. | S0016 | | |
| Diagnosing connectivity problems | S0033 | | |
| Maintaining directory services | S0043 | | |
| Using virtual machines | S0073 | | |
| Configuring and utilizing software-based computer protection tools (e.g. software firewalls, anti-virus software, anti-spyware) | S0076 | | |
| | S0111 | | |
| Conducting system and server planning, management and maintenance | S0143 | | |
| Correcting physical and technical problems that impact system/server performance | S0144 | | |
| Troubleshooting failed system components (i.e. servers) | S0151 | | |
| Identifying and anticipating system/server performance, availability, capacity or configuration problems | S0153 | | |
| Installing system and component upgrades | S0154 | | |
| Monitoring/optimizing system/server performance | S0155 | | |
| Recovering failed systems | S0157 | | |
| Operating system administration | S0158 | | |
| Knowledge & Understanding | 50150 | | |
| See K0001 - K0006 from job function 1 | K0001-K0006 | | |
| | K0033 | | |
| , , | K0040 | | |
| , , | K0040 K0047 | | |
| | K0047 K0049 | | |
| | K0053 | | |
| | K0055 | | |
| Performance tuning tools and techniques | K0050 | | |
| Policy-based and risk-adaptive access controls | K0065 | | |
| Capabilities and functionality associated with various technologies for organizing and managing information | K0005 | | |
| Capabilities and functionality of collaborative technologies | K0096 | | |
| Server and client operating systems | K0077 | | |
| | K0078 | | |
| | K0088 | | |
| Enterprise information technology architecture | K0100 | | |
| Virtual Private Network (VPN) security | K0104 | | |
| File system implementations (e.g. New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]) | | | |
| | K0158 | | |
| Basic system administration, network and operating system hardening techniques | K0167 | | |
| | K0179 | | |
| Transmission records and jamming techniques that enable transmission of undesirable information or prevent installed systems from operating correctly | K0181 | | |
| | K0195 | | |
| - | K0210 | | |
| | K0210 | | |
| | K0211 K0260 | | |
| | K0260 | Optional | |
| · · · · · · · · · · · · · · · · · · · | K0261 | Optional | |
| | K0202 | Sptional | |
| | | | |
| | K0284 | | |
| Organization's information classification program and procedures for information compromise System/server diagnostic tools and fault identification techniques | K0287 | | |
| Nystem/server diagnostic tools and fault identification techniques | K0289 | | |

| | 1 | | 1 |
|--|--------------|----------|----------|
| Tools & Technologies | | | |
| Tools & Technologies | | | |
| Servers | | | |
| Desktop/laptop computers | | | |
| Personal Communication Devices | | | |
| Diagnostic tools and software | | | |
| Database software | | | |
| Networking tools | | | |
| Competency a: Checks system hardware availability, functionality, integrity and efficiency | T0431 | Core | Intermed |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency b: Conducts functional and connectivity testing to ensure continuing operability | T0029 | Core | Basic |
| Competency 6. Conducts functional and connectivity testing to ensure continuing operating | 10029 | Core | Basic |
| | | | |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency c: Conducts periodic server maintenance including cleaning (physically and electronically), | T0435 | Core | Basic |
| disk checks, system configuration and monitoring, data downloads, backups and testing | | | |
| Performance Standards | | | • |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency d: Assists in the development of group policies and access control lists to ensure | T0054 | Optional | Advance |
| Competency d: Assists in the development of group policies and access control lists to ensure compatibility with organizational standards, business rules and needs | T0054 | Optional | Advance |
| | T0054 | Optional | Advance |
| Competency d: Assists in the development of group policies and access control lists to ensure compatibility with organizational standards, business rules and needs Performance Standards | T0054 | Optional | Advance |
| | T0054 | Optional | Advance |
| Performance Standards | | | |
| Performance Standards Competency e: Documents compliance with or changes to system administration standard operating | T0054 T0063 | Optional | |
| Performance Standards Competency e: Documents compliance with or changes to system administration standard operating procedures | | | |
| Performance Standards Competency e: Documents compliance with or changes to system administration standard operating | | | |
| Performance Standards Competency e: Documents compliance with or changes to system administration standard operating procedures | | | |
| Performance Standards Competency e: Documents compliance with or changes to system administration standard operating procedures | | | |
| Performance Standards Competency e: Documents compliance with or changes to system administration standard operating procedures | | | |
| Performance Standards Competency e: Documents compliance with or changes to system administration standard operating procedures | | | |
| Performance Standards Competency e: Documents compliance with or changes to system administration standard operating procedures | | | |
| Performance Standards Competency e: Documents compliance with or changes to system administration standard operating procedures | | | Advance |

| Competency f: Installs server fixes, updates and enhancements | T0418 | Core | Intermediate |
|---|--------------------------|------|----------------|
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency g: Maintains baseline system security according to organizational policies | T0136 | C | Intermediate |
| | 10136 | Core | Intermediate |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency h: Manages accounts, network rights and access to systems and equipment | T0144 | Core | Basic |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Commenter in Manifester and an interior and in the company of the | TO 400 /TO 501 | C | T., 4 1: - 4 - |
| Competency i: Monitors and maintains server configuration | T0498/T0501 | Core | Intermediate |
| Competency i: Monitors and maintains server configuration Performance Standards | T0498/T0501 | Core | Intermediate |
| | Т0498/Т0501 | Core | Intermediate |
| | T0498/T0501 | Core | Intermediate |
| Performance Standards | T0498/T0501 | Core | Intermediate |
| | T0498/T0501 | Core | Intermediate |
| Performance Standards | T0498/T0501 | | |
| Performance Standards Competency j: Supports network components | T0498/T0501 | | |
| Performance Standards Competency j: Supports network components | T0498/T0501 | | |
| Performance Standards Competency j: Supports network components | T0498/T0501 | | |
| Performance Standards Competency j: Supports network components | T0498/T0501 | | |
| Performance Standards Competency j: Supports network components | T0498/T0501 | | |
| Performance Standards Competency j: Supports network components | T0498/T0501 | | |
| Performance Standards Competency j: Supports network components Performance Standards Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to | T0498/T0501 T0514/T0515 | | |
| Performance Standards Competency j: Supports network components Performance Standards Competency Standards Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs | | Core | Basic |
| Performance Standards Competency j: Supports network components Performance Standards Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to | | Core | Basic |
| Performance Standards Competency j: Supports network components Performance Standards Competency Standards Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs | | Core | Basic |
| Performance Standards Competency j: Supports network components Performance Standards Competency Standards Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs | | Core | Basic |
| Performance Standards Competency j: Supports network components Performance Standards Competency Standards Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs | | Core | Basic |
| Performance Standards Competency j: Supports network components Performance Standards Competency Standards Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs | | Core | Basic |
| Performance Standards Competency j: Supports network components Performance Standards Competency Standards Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs | | Core | Basic |

| C | Competency I: Verifies data redundancy and system recovery procedures | T0186 | Core | Intermediate |
|---|---|-------|----------|--------------|
| P | Performance Standards | | | |
| - | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| C | Competency m: Assists in the coordination or installation of new or modified hardware, operating | T0507 | Core | Intermediate |
| | ystems and other baseline software Performance Standards | | | |
| | Citornance Standards | | | |
| | | | | |
| - | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Competency n: Provides ongoing optimization and problem-solving support | T0207 | Core | Intermediate |
| P | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| C | Competency o: Resolves hardware/software interface and interoperability problems | T0531 | Core | Basic |
| P | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| C | Competency p: Establishes adequate access controls based on principles of least privilege, role based | T0475 | Optional | Advanced |
| a | access controls (RBAC) and need-to-know | | ~ P | |
| P | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| RELATED INSTRUCTION | NICE | Core/Optional | LEVE |
|--|----------------|---------------|---------|
| Skills | Framework | | |
| K0001-K0006 from job function 1 | | | |
| Applying host/network access controls (e.g. access control list) | S0007 | | |
| | | | |
| Virtual private network devices and encryption Securing network communication | S0059 | | |
| • | S0077 | | |
| Protecting a network against malware System, network and OS hardening techniques | S0079 S0121 | | |
| Troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution | S0124 | | |
| | | | |
| Knowledge & Understanding | | | |
| K001-K0006 from job function 1 | | | |
| Knowledge of application vulnerabilities | K0009 | | |
| Knowledge of data backups, types of backups and recovery concepts and tools | K0021 | | |
| Host/network access control mechanisms (e.g. access control list) | K0033 | | |
| Cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation) | K0044 | | |
| Virtual private network security | K0104 | | |
| Web filtering technologies | K135 | | |
| Cyberdefense policies, procedures and regulations | K0157 | | |
| Current and emerging cyber technology | K0335 | | |
| Intrusion detection systems, intrusion prevention system tools and applications | K0324 | | |
| Tools & Technologies | | | |
| Networking tools and software | | | |
| Intrusion detection software | | | |
| Virtual Private Network technologies | | | |
| Web filtering technologies | | | |
| Servers and back-up systems | | | |
| | | | |
| TENCIES | | | |
| Competency a: Installs and maintains cyber security detection, monitoring and threat management software | T0485 | Core | Interme |
| Performance Standards | | _ | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency b: Coordinates with network administrators to administer the updating of rules and | T0042 | Core | Interme |
| signatures for intrusion/detection protection systems, anti-virus and network black and white list | 10012 | | |
| Performance Standards | | _ | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| Competency d: Ensures application of security patches for commercial products integrated into system design | T0554 | Core | Basic |
|---|-------|----------|----------|
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency e: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity | T0023 | Optional | Advanced |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| RELATED INSTRUCTION | NICE | Core/Optional | LEVEL |
|--|-------------|---------------|---------|
| Skills | Framework | | |
| Detecting host and network based intrusions via intrusion detection technologies (e.g. snort) | S0025 | | |
| | | | |
| Applying security system access controls | S0031 | | |
| Mimicking threat behavior | S0044 | | |
| Use of penetration tools and technologies | S0051 | | |
| Determining how changes in conditions, operations or the environment will affect these outcomes | S0027 | | |
| Evaluating the adequacy of security designs | S0036 | | |
| Assessing security system designs | S0141 | | |
| | | | |
| Assessing security controls based on cybersecurity principles and trends | S0148 | | |
| Recognizing vulnerabilities in security system | S0167 | | |
| Knowledge & Understanding | | | |
| K0001-K0006 from job function 1 | | | |
| Knowledge list from Job funtion 2: networks | | | |
| Hacking methodologies in Windows or Unix/Linus environment | K0119 | | |
| Network traffic analysis | K334 | | |
| Access authentication methods | K336 | | |
| Penetration testing principles, tools and techniques | K0342 | | |
| Hacking methodologies | K0310 | | |
| Policy based and risk adjusted access controls | K0065 | | |
| Threat environments | K0344 | | |
| Tools & Technologies | | | |
| Penetration tools | | | |
| Authentication devices | | | |
| Windows/Unix/Linux operating systems | | | |
| Network traffic monitoring tools | | | |
| Servers | | | |
| Backup systems | | | |
| ETENCIES | | | |
| Competency a: Applies security policies to meet security objectives of the system | T0016/T0438 | Core | Interme |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices | T0180/T0086 | Core | Interme |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |

| Competency c: Ensures that data back up and restoration systems are functional and consistent with | T0186/T0050 | Core | Basic |
|--|-------------|----------|------------|
| company's document retention policy and business continuity needs | 10100/10050 | | Busic |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency d: Identifies potential conflicts with implementation of any computer network defense tools | T0504 | Optional | Advanced |
| Performs tool signature testing and optimization Performance Standards | | | |
| 1 ciromance bandards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency e: Installs, manages and updates intrusion detection system | T0309 | Optional | Advanced |
| Performance Standards | | | |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency f: Performs technical and non-technical risk and vulnerability assessments of relevant | T0549/T0178 | Optional | Advanced |
| technology focus areas | | * | |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Compatonay as Conducts outhorized non-testion testing (Wi Figure 1) | T0051/T0252 | Coro | Intown - J |
| Competency g: Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results | 10051/10252 | Core | Intermedia |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency h: Documents systems security operations and maintenance activities | T0470 | Core | Intermedia |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |

| Competency i: Communicates potential risks or vulnerabilities to manager. Collaborates with others to recommend vulnerability corrections | T0178 | Optional | Advanced |
|---|-------|----------|----------|
| Performance Standards | | _ | _ |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency j: Identifies information technology security program implications of new technologies or technology upgrades | T0115 | Optional | Advanced |
| Performance Standards | - | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| RELATED INSTRUCTION | NICE Framework | Core/Optional | LEVEL |
|---|-------------------|---------------|--------|
| Skills | Tamework | | |
| Conducting vulnerability scans | S0001 | | |
| Identifying, capturing and containing malware | S0003 | | |
| Applying host/network access controls | S0007 | | |
| | S0139 | | |
| Applying security models | | | |
| Reviewing logs to identify evidence of past intrusions | S0120 | | |
| Outlier identification and removal techniques | S0129 | | |
| Secure test plan design | S0135 | | |
| Developing and deploying signatures | S0020 | | |
| Conducting trend analysis | S0169 | | |
| Recognizing and interpreting malicious network activity in traffic | S0258 | | |
| | | | |
| Mimicking threat behavior | S0044 | | |
| Knowledge & Understanding | | | |
| Application vulnerabilities | K0009 | | |
| Data backups, types of backups and recovery concepts and tools | K0003 | | |
| Disaster recovery continuity of operations plans | K0021 | | |
| | | | |
| Host access control mechanisms | K0033 | | |
| Incident categories, indicent responses and timelines for responses | K0041 | | |
| Intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies | K0046 | | |
| Network traffic analysis techniques | K0058 | | |
| Packet analysis | K0062 | | |
| Privacy impact assessment methodologies | K0062 K0066 | | |
| | | | |
| Incident response and handling methodologies | K0042 | | |
| Tools & Technologies | | | |
| Data backup tools and technologies | | | |
| Networking devices | | | |
| Network traffic detection devices | | | |
| Intrusion detection technologies | | | |
| Software/Applications of relevance to organization | | | |
| Malware | | | |
| ETENCIES | | | |
| Competency a: Identifies organizational trends with regard to the security posture of systems; identifies | T0198 | Core | Basic |
| unusual patterns or activities | | | |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency b: Characterizes and analyzes network traffic to identify anomalous activity and potential threats; performs computer network defense trend analysis and reporting | T0333 | Optional | Advano |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| Competency c: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | T0043/T0214 | Optional | Advanced |
|--|--------------|----------|--------------|
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency d: Runs tests to detect real or potential threats, viruses, malware, etc. | T2096/T2097 | Optional | Advanced |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency e: Assists in researching cost-effective security controls to mitigate risks | T0550/T0310/ | Core | Intermediate |
| Competency C. Pissists in researching cost effective security controls to integrate risks | T0088/T0503 | Core | |
| Performance Standards | • | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | - | | |
| | | | |
| | | | |
| | | | |
| Competency f: Helps perform damage assessments in the event of an attack | | Optional | Advanced |
| Competency f: Helps perform damage assessments in the event of an attack Performance Standards | | Optional | Advanced |
| | | Optional | Advanced |
| Performance Standards | TOLICA | | |
| | T0164 | Optional | Advanced |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other | T0164 | | |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities | T0164 | | |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities | T0164 | | |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities | T0164 | | |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities | T0164 | | |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities | T0164 | | |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities | T0164 | | |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities Performance Standards | | Optional | Advanced |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities | T0164 T0155 | | |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities Performance Standards Competency h: Documents and escalates incidents that may cause immediate or long-term impact to the | | Optional | Advanced |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities Performance Standards Competency h: Documents and escalates incidents that may cause immediate or long-term impact to the environment | | Optional | Advanced |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities Performance Standards Competency h: Documents and escalates incidents that may cause immediate or long-term impact to the environment | | Optional | Advanced |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities Performance Standards Competency h: Documents and escalates incidents that may cause immediate or long-term impact to the environment | | Optional | Advanced |
| Performance Standards Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities Performance Standards Competency h: Documents and escalates incidents that may cause immediate or long-term impact to the environment | | Optional | Advanced |

| Competency i: Provides timely detection, identification and alerts of possible attacks and intrusions, anomalous activities, and distinguish these incidents and events from normal baseline activities | T0258/T0214 | Optional | Advanced |
|---|-------------|----------|----------|
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency j: Uses network monitoring tools to capture and analyze network traffic associated with malicious activity | T0259 | Optional | Advanced |
| Performance Standards | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Competency k: Performs intrusion analysis | T0169 | Optional | Advanced |
| Competency k: Performs intrusion analysis Performance Standards | T0169 | Optional | Advanced |
| | T0169 | Optional | Advanced |
| Performance Standards | | | |
| | T0169 | Optional | |
| Performance Standards Competency 1: Sets containment blockers to align with company policy regarding computer use and web | | | Advanced |
| Performance Standards Competency 1: Sets containment blockers to align with company policy regarding computer use and web access | | | |
| Performance Standards Competency 1: Sets containment blockers to align with company policy regarding computer use and web access | | | |
| Performance Standards Competency 1: Sets containment blockers to align with company policy regarding computer use and web access | | | |
| Performance Standards Competency 1: Sets containment blockers to align with company policy regarding computer use and web access | | | |
| Performance Standards Competency 1: Sets containment blockers to align with company policy regarding computer use and web access | | | |
| Performance Standards Competency 1: Sets containment blockers to align with company policy regarding computer use and web access | | | |
| Performance Standards Competency 1: Sets containment blockers to align with company policy regarding computer use and web access | | | |
| Performance Standards Competency 1: Sets containment blockers to align with company policy regarding computer use and web access | | | |

| F | ELATED INSTRUCTION | NICE | Core/Optional | LEVEL |
|--------|--|-----------|---------------|----------|
| S | kills | Framework | | |
| h | Troubleshooting failed system components | T0150 | | |
| | Developing, testing and implementing network infrastructure contingency and recovery plans | S0032 | | |
| | acket-level analysis using appropriate tools (e.g. wireshart, tcpdump) | S0046 | | |
| | reserving evidence integrity according to standard operating procedures or national standards | S0047 | | |
| | analyzing memory dumps to extract information | S0062 | | |
| I (| dentifying, modifying and manipulationg applicable system components within Windows, Unix or Linus e.g. passwords, user accounts, files) | S0067 | | |
| Ţ | Jsing forensic tools suites (e.g. EnCase, Sleuthkit, FTK) | S0071 | | |
| | hysically disassembling PCs | S0074 | | |
| k | nowledge & Understanding | | | |
| | (0001-K0006(see job function 1) | K0001-6 | | |
| | Concepts and practices for processing digital forensic data | K0017 | | |
| | Data backups, types of backups and recovery concepts and tools | K0021 | | |
| L | neident response and handling methodologies | K0042 | | |
| 0 | Operating systems | K0060 | | |
| S | erver diagnostic tools and fault identification techniques | K0078 | | |
| F | rocess for seizing and preserving digital evidence (e.g. chain of custody) | K0118 | | † |
| | Web mail collection, searching/analyzing techniques, tools and cookies | K0131 | | |
| S | ystem files (log files, registry files, configuration files) contain relevant information and where to find nose system files | K0131 | | |
| | ypes of digital forensics data and how to recognize them | K0133 | | |
| | Virtual machine aware malware, debugger aware malware and packing | K0199 | | |
| ш | | | | |
| | ystem and application security threats and vulnerabilities cols & Technologies | K0070 | | |
| L | | | | |
| | Vireshark Tcpdump | | | |
| _ | nCase, Sleuthkit, FTK | | | |
| ш | | | | - |
| | ecurity event correlation tools orensic tools such as Wireshark and VMWare | | | |
| | Allware analysis tools (Oily Debug, Ida Pro) | | | _ |
| | TENCIES | | | |
| | Competency a: Assists in the development of appropriate courses of action in response to identified | T0295 | Optional | Advanc |
| | nomalous network activity erformance Standards | | | |
| 1 | Cromance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| (| Competency b: Triages systems operations impact: malware, worms, man-in-the-middle attack, denial of | T0504 | Optional | Advanc |
| S | ervice, rootkits, keystroke loggers, SQL injection and cross-site scripting | 10304 | - Optional | Auvano |
| F | erformance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| f | | T0298 | Optional | Advance |

| O | Competency d: Correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation | T0260/T0292 | Optional | Advanced |
|---|--|-------------|----------|----------|
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | T0166/T0167 | 0 1 | A 1 1 |
| О | Competency e: Monitors external data sources to maintain currency of Computer Network Defense threat condition and determines which security issues may have an impact on the enterprise. Performs file signature analysis | 10166/1016/ | Optional | Advanced |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| _ | Competency f: Performs analysis of log files from a variety of sources to identify threats to network | T0433/T0167 | Optional | Advanced |
| О | security; performs file signature analysis | 10133/1010/ | optional | Auvanceu |
| 0 | security; performs file signature analysis Performance Standards | 10133/1010/ | | Advanced |
| 0 | security; performs file signature analysis | 10133/1010/ | | Auvanceu |
| 0 | security; performs file signature analysis | 10133,10107 | | Advanced |
| | security; performs file signature analysis | 10133110101 | | Advanced |
| | security; performs file signature analysis | 10103110101 | | Auvanced |
| | security; performs file signature analysis | 10.03.10101 | | Auvanced |
| | security; performs file signature analysis | 10103110101 | | Auvanced |
| | security; performs file signature analysis | | | Advanced |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | | Optional | Advanced |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes | | | |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | | | |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | | | |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | | | |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | | | |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | | | |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | | | |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | | | |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation | | | |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation Performance Standards Competency h: Receives and analyzes network alerts from various sources within the enterprise and | T0047 | Optional | Advanced |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation Performance Standards Competency h: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | T0047 | Optional | Advanced |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation Performance Standards Competency h: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | T0047 | Optional | Advanced |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation Performance Standards Competency h: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | T0047 | Optional | Advanced |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation Performance Standards Competency h: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | T0047 | Optional | Advanced |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation Performance Standards Competency h: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | T0047 | Optional | Advanced |
| 0 | Security; performs file signature analysis Performance Standards Competency g: Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes recommendations that enable expeditious remediation Performance Standards Competency h: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts | T0047 | Optional | Advanced |

| С | Competency i: Tracks and documents computer network defense incidents from initial detection through final resolution | T0395/T0233/ | Core | Intermediate |
|---|--|--------------|----------|--------------|
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | T0250 | 0 : 1 | |
| О | Competency j: Collects intrusion artifacts and uses discovered data to enable mitigation of potential computer network defense (CND) incidents | T0278 | Optional | Advanced |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Competency ly Donforms views soonning on digital modic | | Core | Basic |
| С | Competency k: Performs virus scanning on digital media | | Core | Basic |
| | Performance Standards | 1 | 1 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| 1 threats | LEVEL | |
|---|--------------------|--|
| Scope | | |
| | | |
| Skills | | |
| | | |
| Developing and deploying signatures | S0020 | |
| Incident handling methodologies | S0054 | |
| Using protocol analyzers Recognizing and categorizing types of vulnerabilities and associated attacks | S0057 | |
| Recognizing and categorizing types of vulnerabilities and associated attacks Reading and interpreting signatures | S0078 S0096 | |
| Assessing security controls based on cybersecurity principles and tenents | S0096 S0147 | |
| Assessing security controls based on cybersecurity principles and tenents | 30147 | |
| Recognizing vulnerabilities in security systems | S0167 | |
| Conducting trend analysis | S0169 | |
| Knowledge & Understanding | | |
| Other defense and uninerability assessment tools including area source tools and their conditions | K0013 | |
| Cyber defense and vulnerability assessment tools, including open source tools, and their capabilities Host/network access control mechanisms | K0013 | |
| Cybersecurity principles used to manage risks related to the use, processing, storage and transmission of | K0033 | |
| information or data | X0038 | |
| Known vulnerabilities from alerts, advisories, errata and bulletins | K0040 | |
| Incident response and handling methodologies | K0042 | |
| Intrusion detection methodologies and techniques for detecting host and network-based intrusions via | K0046 | |
| intrusion detection technologies | Wolce | |
| Elements of a network attack and the relationship to both threats and vulnerabilities | K0106 | |
| Common network tools (e.g. ping, traceroute, nslookup) and interpret the information results | K0111 | |
| Encryption methodologies Countermeasure design for identified security risks | K0190 K0298 | |
| Countermeasure design for identified security fisks | K0296 | |
| | | |
| | 770454 | |
| Different classes of attacks (e.g. passive, active, insider, close-in, distribution) | K0161 | |
| Different classes of attacks (e.g. passive, active, insider, close-in, distribution) Tools & Technologies | K0161 | |
| | K0161 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify | K0161 T0469/T0470 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities Performance Standards | T0469/T0470 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities | | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities Performance Standards Competency b: Characterize and analyze network traffic to identify anomalous activity and potential threats; perform computer network defense trend analysis and reporting | T0469/T0470 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities Performance Standards Competency b: Characterize and analyze network traffic to identify anomalous activity and potential threats; perform computer network defense trend analysis and reporting | T0469/T0470 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities Performance Standards Competency b: Characterize and analyze network traffic to identify anomalous activity and potential threats; perform computer network defense trend analysis and reporting | T0469/T0470 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities Performance Standards Competency b: Characterize and analyze network traffic to identify anomalous activity and potential | T0469/T0470 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities Performance Standards Competency b: Characterize and analyze network traffic to identify anomalous activity and potential threats; perform computer network defense trend analysis and reporting | T0469/T0470 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities Performance Standards Competency b: Characterize and analyze network traffic to identify anomalous activity and potential threats; perform computer network defense trend analysis and reporting | T0469/T0470 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities Performance Standards Competency b: Characterize and analyze network traffic to identify anomalous activity and potential threats; perform computer network defense trend analysis and reporting | T0469/T0470 | |
| Tools & Technologies Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities Performance Standards Competency b: Characterize and analyze network traffic to identify anomalous activity and potential threats; perform computer network defense trend analysis and reporting | T0469/T0470 | |

| Core or Optional | Competency c: Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts | T0214 | |
|---------------------|--|-------------|--|
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency d: Run tests to detect real or potential threats, viruses, malware, etc. | T0296/T0295 | |
| Optional | | 10270/10273 | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency e: Assists in researching cost-effective security controls to mitigate risks | T0310/T0550 | |
| Optional | | | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency f: Perform damage assessments in the event of an attack | | |
| | Performance Standards | | |
| | 1 cromance standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| _ | | | |
| Core or Optional | Competency g: | | |
| | Performance Standards | | |
| | 1 CHOIMAINCE STAINGARD | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency h: | | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| Core or Optional | Competency i: | | |
|---------------------|-----------------------|--|--|
| Optional | | | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency j: | | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| Job Fun | ction: | LEVEL | OJT | RI |
|---------------------|---------------------------|-------|-----|----|
| | Scope | | | |
| | | | | |
| | Skills | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Knowledge & Understanding | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Tools and Technologies | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or Optional | Competency a: | | | |
| | | | | |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or Optional | Competency b: | | | |
| | | | | |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or Optional | Competency c: | | | |
| | | | | |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or Optional | Competency d: | | | |
| | | | | |

| | Performance Standards | | |
|---------------------|--------------------------------------|--|--|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency e: | | |
| | | | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency f: | | |
| | | | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or | Competency g: | | |
| Core or Optional | Competency g. | | |
| | Performance Standards | | |
| | 1 0110111MILOU DIMINUM | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency h: | | |
| | | | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency i: | | |
| Optional | | | |
| Optional | Competency i: Performance Standards | | |
| Optional | | | |

| Core or Optional | Competency j: | | |
|---------------------|-----------------------|--|--|
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| Performance Standards | Job Fun | | LEVEL | OJT | RI |
|--|---------------------|--|-------|-----|----|
| Knowledge & Understanding Knowledge & Understanding Contributions Competency a: Performance Standards Competency b: Performance Standards Performance Standards Performance Standards Performance Standards Performance Standards Performance Standards | | Scope | | | |
| Knowledge & Understanding Knowledge & Understanding Contributions Competency a: Performance Standards Competency b: Performance Standards Performance Standards Performance Standards Performance Standards Performance Standards Performance Standards | | | | | |
| Certifications Competency a: Performance Standards Competency b: Competency b: Competency b: Competency c: Competency c: Performance Standards | | Skills | | | |
| Certifications Competency a: Performance Standards Competency b: Competency b: Competency b: Competency c: Competency c: Performance Standards | | | | | |
| Certifications Competency a: Performance Standards Competency b: Competency b: Competency b: Competency c: Competency c: Performance Standards | | | | | |
| Certifications Competency a: Performance Standards Competency b: Competency b: Competency b: Competency c: Competency c: Performance Standards | | | | | |
| Certifications Competency a: Performance Standards Competency b: Competency b: Competency b: Competency c: Competency c: Performance Standards | | | | | |
| Certifications Competency a: Performance Standards Competency b: Competency b: Competency b: Competency c: Competency c: Performance Standards | | | | | |
| Certifications Competency a: Performance Standards Competency b: Competency b: Competency b: Competency c: Competency c: Performance Standards | | | | | |
| Certifications Competency a: Performance Standards Competency b: Competency b: Competency b: Competency c: Competency c: Performance Standards | | | | | |
| Competency b: Performance Standards Competency b: Performance Standards Performance Standards Performance Standards Performance Standards | | Knowledge & Understanding | | | |
| Competency b: Performance Standards Competency b: Performance Standards Performance Standards Performance Standards Performance Standards | | | | | |
| Competency b: Performance Standards Competency b: Performance Standards Performance Standards Performance Standards Performance Standards | | | | | |
| Competency b: Performance Standards Competency b: Performance Standards Performance Standards Performance Standards Performance Standards | | | | | |
| Competency b: Performance Standards Competency b: Performance Standards Performance Standards Performance Standards Performance Standards | | | | | |
| Competency b: Performance Standards Competency b: Performance Standards Performance Standards Performance Standards Performance Standards | | | | | |
| Performance Standards Competency b: Performance Standards Competency c: Performance Standards | | Certifications | | | |
| Performance Standards Competency b: Performance Standards Competency c: Performance Standards | | | | | |
| Performance Standards Competency b: Performance Standards Competency c: Performance Standards | | | | | |
| Performance Standards Competency b: Performance Standards Competency c: Performance Standards | | | | | |
| Performance Standards Competency b: Performance Standards Competency c: Performance Standards | | | | | |
| Performance Standards Competency b: Performance Standards Competency c: Performance Standards | Core or | Compared to the control of the contr | | | |
| Competency b: Performance Standards Competency c: Performance Standards | Optional | Competency a: | | | |
| Performance Standards Competency c: Performance Standards Performance Standards Outpitional Competency c: Performance Standards | | Performance Standards | | | |
| Performance Standards Competency c: Performance Standards Performance Standards Outpitional Competency c: Performance Standards | | | | | |
| Performance Standards Competency c: Performance Standards Performance Standards Outpitional Competency c: Performance Standards | | | | | |
| Performance Standards Competency c: Performance Standards Performance Standards Outpitional Competency c: Performance Standards | | | | | |
| Performance Standards Competency c: Performance Standards Performance Standards Outpitional Competency c: Performance Standards | | | | | |
| Performance Standards Competency c: Performance Standards Performance Standards Outpitional Competency c: Performance Standards | | | | | |
| Performance Standards Competency c: Performance Standards Performance Standards Outpitional Competency c: Performance Standards | | | | | |
| Performance Standards Competency c: Performance Standards Performance Standards Outpitional Competency c: Performance Standards | Core or Optional | Competency b: | | | |
| Competency c: Performance Standards | | | | | |
| Performance Standards | | r criorinance Standards | | | |
| Performance Standards | | | | | |
| Performance Standards | | | | | |
| Performance Standards | | | | | |
| Performance Standards | | | | | |
| Performance Standards | | | | | |
| Performance Standards | Com | | | | |
| | Core or Optional | Competency c: | | | |
| | | Performance Standards | | | |
| Core or Competency d: | | | | | |
| Core or Competency d: | | | | | |
| Competency d; | | | | | |
| Core or Optional Competency d: | | | | | |
| Core or Competency d: | | | | | |
| Core or Optional Competency d: | | | | | |
| puonal 1 | Core or | Competency d: | | | |
| | Optional | | | | |

| | Performance Standards | | |
|---------------------|--|--|--|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Core or Optional | Competency e: | | |
| | | | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| 0 | | | |
| Core or Optional | Competency f: | | |
| | | | |
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | (Competency a: | | |
| Optional | Competency g: | | |
| | | | |
| | Performance Standards | | |
| | | | |
| • | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | Performance Standards | | |
| | | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards Competency h: Performance Standards | | |
| Core or Optional | Performance Standards Competency h: Performance Standards | | |
| Core or Optional | Performance Standards Competency h; | | |
| Core or Optional | Performance Standards Competency h: Performance Standards Competency i: | | |
| Core or Optional | Performance Standards Competency h: Performance Standards | | |
| Core or Optional | Performance Standards Competency h: Performance Standards Competency i: | | |
| Core or Optional | Performance Standards Competency h: Performance Standards Competency i: | | |
| Core or Optional | Performance Standards Competency h: Performance Standards Competency i: | | |
| Core or Optional | Performance Standards Competency h: Performance Standards Competency i: | | |
| Core or Optional | Performance Standards Competency h: Performance Standards Competency i: | | |
| Core or Optional | Performance Standards Competency h: Performance Standards Competency i: | | |
| Core or Optional | Performance Standards Competency h: Performance Standards Competency i: | | |

| Core or Optional | Competency j: | | |
|---------------------|-----------------------|--|--|
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| Job Fun | ction : | LEVEL | OJT | RI |
|---------------------|---------------------------|-------|-----|----|
| | Scope | | | |
| | | | | |
| | | | | |
| | Skills | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Knowledge & Understanding | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Toos & Technologies | | | |
| | 1008 & Techniologies | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or Optional | Competency a: | | | |
| | | | | |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or Optional | Competency b: | | | |
| Орионы | | | | |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or | Competency c: | | | |
| Core or Optional | Competency C. | | | |
| | Performance Standards | | | |
| | 1 CHOITHAIRCE Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or | | | | |
| Core or Optional | Competency d: | | | |
| | | | | |

| | Performance Standards | | | | |
|---------------------|--|--|--|--|--|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Core or Optional | Competency e: | | | | |
| | | | | | |
| | Performance Standards | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Core or Optional | Competency f: | | | | |
| , | | | | | |
| | Performance Standards | | | | |
| | - Constitution State and Constitution Consti | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Core or Optional | Competency g: | | | | |
| Optional | F 3 D | | | | |
| | Performance Standards | | | | |
| | renominate standards | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Core or Optional | Competency h: | | | | |
| Optional | competency ii. | | | | |
| | Darformanaa Standarda | | | | |
| | Performance Standards | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Core or | Compatancy is | | | | |
| Core or Optional | Competency i: | | | | |
| | | | | | |
| | Competency i: Performance Standards | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| Core or Optional | Competency j: | | |
|---------------------|-----------------------|--|--|
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| Job Fun | ction : | LEVEL | OJT | RI |
|---------------------|---------------------------|-------|-----|----|
| | Scope | | | |
| | | | | |
| | | | | |
| | Skills | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Knowledge & Understanding | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Tools & Technologies | | | |
| | Tools & Toolstog to | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or | | | | |
| Core or Optional | Competency a: | | | |
| | | | | |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| _ | | | | |
| Core or Optional | Competency b: | | | |
| | | | | |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or Optional | Competency c: | | | |
| | | | | |
| | Performance Standards | | | |
| | | | | |
| | | | | |
| ĺ | | | | |
| İ | | | | |
| İ | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Core or Optional | Competency d: | | | |
| Optional | | | | |

| | Performance Standards | | | | | |
|---------------------|--|--|--|--|--|--|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Core or Optional | Competency e: | | | | | |
| | | | | | | |
| | Performance Standards | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Core or Optional | Competency f: | | | | | |
| | | | | | | |
| | Performance Standards | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Core or | Competency g: | | | | | |
| Core or Optional | Competency g. | | | | | |
| | Performance Standards | | | | | |
| | To the state of th | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Core or Optional | Competency h: | | | | | |
| | | | | | | |
| | Performance Standards | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Core or Optional | Competency i: | | | | | |
| Optional | | | | | | |
| Optional | Competency i: Performance Standards | | | | | |
| Optional | | | | | | |
| Optional | | | | | | |
| Optional | | | | | | |
| Optional | | | | | | |
| Optional | | | | | | |
| Optional | | | | | | |
| Optional | | | | | | |

| Core or Optional | Competency j: | | |
|---------------------|-----------------------|--|--|
| | Performance Standards | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |