COMPETENCY-BASED OCCUPATIONAL FRAMEWORK FOR REGISTERED APPRENTICESHIP

Cyber Security Support Technician

ONET Code: 15.1122

RAPIDS Code: 2050CB

Created: August 2017

Updated: December 2017

This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment and Training Administration under Contract Number DOL-ETA-15-C-0087. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of the same by the U.S. Government.

For More Information, Contact:

Diana Elliott, PhD, Senior Research Associate, Urban Institute: delliott@urban.org

Robert Lerman, PhD, Institute Fellow, Urban Institute: rlerman@urban.org

URBAN INSTITUTE · ELEVATE · THE · DEBATE

Acknowledgments

We thank Diane Auer Jones for her expertise and contributions to this document.

Contents

Competency-Based Occupational Frameworks

The Urban Institute, under contract by the U.S. Department of Labor, has worked with employers, subject matter experts, labor unions, trade associations, credentialing organizations and academics to develop Competency-Based Occupational Frameworks (CBOF) for Registered Apprenticeship programs. These frameworks defined the **purpose** of an occupation, the **job functions** that are carried out to fulfill that purpose, the **competencies** that enable the apprentice to execute those job functions well, and the **performance criteria** that define the specific knowledge, skills and personal attributes associated with high performance in the workplace. This organizational hierarchy – Job Purpose – Job Functions – Competencies – Performance Criteria – is designed to illustrate that performing work well requires more than just acquiring discrete knowledge elements or developing a series of manual skills. To perform a job well, the employee must be able to assimilate knowledge and skills learned in various settings, recall and apply that information to the present situation, and carry out work activities using sound professional judgment, demonstrating an appropriate attitude or disposition, and achieving a level of speed and accuracy necessary to meet the employer's business need.

The table below compares the terminology of Functional Analysis with that of traditional Occupational Task Analysis to illustrate the important similarities and differences. While both identify the key technical elements of an occupation, Functional Analysis includes the identification of behaviors, attributes and characteristics of workers necessary to meet an employer's expectations.

Framework Terminology	Traditional Task Analysis Terminology
Job Function – the work activities that are carried out to fulfill the job purpose	Job Duties – roles and responsibilities associated with an occupation
Competency – the actions an individual takes and the attitudes he/she displays to complete those activities	Task – a unit of work or set of activities needed to produce some result
Performance Criteria – the specific knowledge, skills, dispositions, attributes, speed and accuracy associated with meeting the employer's expectations	Sub Task – the independent actions taken to perform a unit of work or a work activity

Although designed for use in competency-based apprenticeship, these Competency-Based Occupational Frameworks also support time-based apprenticeship by defining more clearly and precisely what the apprentice is expected to learn and do during the allocated time-period.

CBOFs are comprehensive in to encompass the full range of jobs that may be performed by individuals in the same occupation. As employers or sponsors develop their individual apprenticeship programs, they can extract from or add to the framework to meet their unique organizational needs.

Components of the Competency-Based Occupational Framework

Occupational Overview: This section of the framework provides a description of the occupation including its purpose, the setting in which the job is performed and unique features of the occupation.

Work Process Schedule: This section includes the job functions and competencies that would likely be included in an apprenticeship sponsor's application for registration. These frameworks provide a point of reference that has already been vetted by industry leaders so sponsors can develop new programs knowing that they will meet or exceed the consensus expectations of peers. Sponsors maintain the ability to customize their programs to meet their unique needs, but omission of a significant number of job functions or competencies should raise questions about whether or not the program has correctly identified the occupation of interest.

Cross-cutting Competencies: These competencies are common among all workers, and focus on the underlying knowledge, attitudes, personal attributes and interpersonal skills that are important regardless of the occupation. That said, while these competencies are important to all occupations, the relative importance of some versus others may change from one occupation to the next. These relative differences are illustrated in this part of the CBOF and can be used to design pre-apprenticeship programs or design effective screening tools when recruiting apprentices to the program.

Detailed Job Function Analysis: This portion of the framework includes considerable detail and is designed to support curriculum designers and trainers in developing and administering the program. There is considerable detail in this section, which may be confusing to those seeking a more succinct, higher-level view of the program. For this reason, we recommend that the Work Process Schedule be the focus of program planning activities, leaving the detailed job function analysis sections to instructional designers as they engage in their development work.

a. Related Technical Instruction: Under each job function appears a list of foundational knowledge, skills, tools and technologies that would likely be taught in the classroom to enable the apprentice's on-the-job training safety and success.

b. Performance Criteria: Under each competency, we provide recommended performance criteria that could be used to differentiate between minimally, moderately and highly competent apprentices. These performance criteria are generally skills-based rather than knowledge-based, but may also include dispositional and behavioral competencies.

Using the Competency-Based Occupational Framework to Develop a Registered Apprenticeship Program

When developing a registered apprenticeship program, the Work Process Schedule included in this CBOF provides an overview of the job functions and competencies an expert peer group deemed to be important to this occupation. The Work Process Schedule in this document can be used directly, or modified and used to describe your program content and design as part of your registration application.

When designing the curriculum to support the apprenticeship program – including on the job training and related technical instruction – the more detailed information in Section 5 could be helpful. These more detailed job function documents include recommendations for the key knowledge and skill elements that might be included in the classroom instruction designed to support a given job function, and the performance criteria provided under each competency could be helpful to trainers and mentors in evaluating apprentice performance and insuring inter-rater reliability when multiple mentors are involved.

Cyber Security Support Technician Occupational Overview

Occupational Purpose and Context

Cyber security professionals work to maintain the security and integrity of information technology systems, networks and devices. According to the National Cybersecurity Workforce Framework, cyber security professionals perform one or more of the following functions: securely provision, operate and maintain, protect and defend, investigate, collect and operate, analyze and provide oversight and development.

Cyber security support technicians and analysts can be employees of small to large companies, non-profits and government agencies, can be outside contractors that provide services to other organizations, and can be self-employed or start their own service company.

Potential Job Titles

Cyber security analyst, cyber security monitor, vulnerability analyst, information systems security analyst, network security analyst

Attitudes and Behaviors

Cyber security support technicians need to be detail oriented, enjoy working with technology, apply logic to solve complex problems and work with a wide range of people, including other technical staff as well as non-technical uses of information technology equipment and systems. These individuals also need to have patience and be able to review large amounts of data to identify and mitigate against potential vulnerabilities or threats.

Apprenticeship Prerequisites

n/a

Occupational Pathways

Cyber security support technicians, with experience and additional certifications, can move into a variety of positions, including security analyst, network security engineer, information systems security manager and information assurance security officer.

Certifications, Licensure and Other Credential Requirements

CREDENTIAL	Offered By	Before, During or After Apprenticeship
CompTia Security+ (Certification)	CompTia	During or After
Certified Information Systems Security Professional (CISSP) (Certification)	(ISC)^2	Requires 5 years of work experience in the security field
Multiple Vendor Certifications available, such as CISCO,		During or After

Job Functions

JOB FUNCTIONS		Core or Optional	Level
1.	Assists in developing security policies and protocols: assists in enforcing company compliance with network security policies and protocols		
2.	Provides technical support to users or customers		
3.	Installs, configures, tests, operates, maintains and manages networks and their firewalls including hardware and software that permit sharing and transmission of information		
4.	Installs, configures, troubleshoots and maintains server configurations to ensure their confidentiality, integrity and availability; also manages accounts, firewalls, configuration, patch and vulnerability management. Is responsible for access control, security configuration and administration		
5.	Configures tools and technologies to detect, mitigate and prevent potential threats		
6.	Assesses and mitigates system network, business continuity and related security risks and vulnerabilities		
7.	Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats		
8.	Responds to cyber intrusions and attacks and provides defensive strategies		

Stackable Programs

This occupational framework is designed to link to the following additional framework(s) as part of a career laddering pathway.

Stackable Programs		Base or Higher Level	Stacks on top of
1.	This program is designed to stack on top of the IT Generalist Framework	Higher Level	IT Generalist

	for those who have little or no prior IT experience.		
2.			
3.			
4.			

Options and Specializations

The following options and specializations have been identified for this occupation. The Work Process Schedule and individual job function outlines indicate which job functions and competencies were deemed by industry advisors to be optional. Work Process Schedules for Specializations are included at the end of this document.

Options and Specializations	Option	Specialization

Levels

Industry advisors have indicated that individuals in this occupation may function at different levels, based on the nature of their work, the amount of time spent in an apprenticeship, the level of skills or knowledge mastery, the degree of independence in performing the job or supervisory/management responsibilities.

Level	Distinguishing Features	Added Competencies	Added Time Requirements

NICE Framework Alignment

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Located in the Information Technology Laboratory at NIST, the NICE Program Office operates under the Applied Cybersecurity Division, positioning the program to support the country's ability to address current and future cybersecurity challenges through standards and best practices.

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure.

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) is a reference structure that describes the interdisciplinary nature of cybersecurity work. It serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization. As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or

provide guidance on different aspects of cybersecurity workforce development, planning, training, and education.

The NICE Framework is available at:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

We have mapped the Competency-Based Occupational Framework for Cyber Security Technician to the NICE framework to ensure that our work is consistent with the lexicon developed by the NICE initiative. The Cyber Security Support Technician role is not one of the occupations specified in the NICE Framework, so our work draws from the introductory level competencies associated with several different specialty occupations within the NICE Framework.

NICE Framework Category: Each of our competencies is mapped to the appropriate Framework Category in the NICE Framework. These categories include:

- SP – Securely Provision
- OM – Operate and Maintain
- OV – Oversee and Govern
- PR – Protect and Defend
- AN – Analyze
- CO – Collect and Operate
- IN - Investigate

NICE Framework Specialty Area: Within each Framework Category are a number of specialty areas that more narrowly define an individual job role or roles. Our Occupational Frameworks include the Specialty Area associated with each of our competencies. For example, within the Category of Securely Provision, there are 7 specialty areas including:

- Risk Management (RSK)
- Software Development (DEV)

- Systems Architecture (ARC)
- Systems Requirements Planning (SRP)
- Technology R&D (TRD)
- Test and Evaluation (TST)
- Systems Development (SYS)

NICE Tasks, Knowledge, Skills and Abilities: We have mapped each of the knowledge, skills, abilities and performance criteria in our Occupational Framework to the appropriate ID number that appears in the NICE Framework tables.

For example:

T0001 is a NICE Task defined as: Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology IIT) security goals and objectives and reduce overall organizational risk.

K0001 is a NICE Framework Knowledge element defined as: Knowledge of computer networking concepts and protocols, and network security methodologies.

S0001 is a NICE Framework Skill Requirement defined as: Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.

A0001 is a NICE Framework Ability Code defined as: Ability to identify systematic security issues based on the analysis of vulnerability and configuration data.

Work Process Schedule

WORK PROCESS SCHEDULE Cyber Security Support Technician		ONET Code: 15.1122 RAPIDS Code: 2050CB
NOTE: This occupational framework has been mapped to the NICE Framework to ensure consistency with the lexicon developed by the NICE working group (https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework)		
JOB TITLE:		
LEVEL:	SPECIALIZATION:	
STACKABLE PROGRAM ___yes _____no **BASE OCCUPATION NAME:**		
Company Contact: Name		
Address:	Phone	Email
Apprenticeship Type: **_____Competency-Based** **_____Time-Based _____Hybrid**		

JOB FUNCTION 1: Assists in developing security policies and protocols; assists in enforcing company compliance with network security policies and protocols	Core or Optional		**Level**
Competencies	Level	NICE Framework Category	NICE Framework Specialty Area
A. Locates (in Intranet, employee handbook or security protocols) organizational policies intended to maintain security and minimize risk and explains their use	Basic	Oversee and Govern	Education and Training
B. Provides guidance to employees on how to access networks, set passwords, reduce security threats and provide defensive measures associated with searches, software downloads,	Advanced	Securely Provision	Information Assurance Compliance

email, Internet, add-ons, software coding and transferred files			
C. Ensures that password characteristics are explained and enforced and that updates are required and enforced based on appropriate time intervals	Basic	Securely Provision	Information Assurance Compliance
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	Intermediate	Oversee and Govern	Education and Training
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	Advanced	Securely Provision	Information Assurance Compliance
F. Assists employees in the use of technologies that restrict or allow for remote access to the organization's information technology network	Intermediate	Oversee and Develop	Education and Training
G. Develops security compliance policies and protocols for external services (i.e. Cloud service providers, software services, external data centers)	Advanced	Securely Provision	Information Assurance Compliance
H. Complies with incident response and handling methodologies	Advanced	Protect and Defend	Computer Network Defense Analysis
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	Intermediate	Securely Provision	System Security Architecture

JOB FUNCTION 2: Provides technical support to users or customers	Core or Optional		Level
Competencies	Level	NICE Framework Category	NICE Framework Specialty Area

A. Manages inventory of IT resources	Basic	Operate/ Maintain	Customer Service and Technical Support
B. Diagnoses and resolves customer-reported system incidents	Intermediate	Investigate	Digital forensics
C. Installs and configures hardware, software and peripheral equipment for system users	Basic	Operate/ Maintain	Customer Service and Technical Support
D. Monitors client-level computer system performance	Basic	Operate/ Maintain	Customer Service and Technical Support
E. Tests computer system performance	Basic	Operate/ Maintain	Customer Service and Technical Support
F. Troubleshoots system hardware and software	Basic	Operate/ Maintain	Customer Service and Technical Support
G. Administers accounts, network rights, and access to systems and equipment	Intermediate	Operate/ Maintain	Customer Service and Technical Support
H. Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines	Advanced	Operate/ Maintain	Systems Security Analysis

JOB FUNCTION 3: Installs, configures, tests, operates, maintains and manages networks and their firewalls including hardware and software that permit sharing and transmission of information	Core or Optional		Level
Competencies	Level	NICE Framework Category	NICE Framework Specialty Area
A. 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

B. Installs, replaces, configures and optimizes network hubs, routers and switches	Advanced	Operate and Maintain	Network Services
C. Assists in network backup and recovery procedures	Intermediate	Operate and Maintain	Network Services
D. Diagnoses network connectivity problems	Basic	Operate and Maintain	Network Services
E. Modifies network infrastructure to serve new purposes or improve workflow	Advanced	Operate and Maintain	Network Services
F. Integrates new systems into existing network architecture	Intermediate	Operate and Maintain	Network Services
G. Patches network vulnerabilities to ensure information is safeguarded against outside parties	Intermediate	Operate and Maintain	Network Services
H. Repairs network connectivity problems	Basic	Operate and Maintain	Network Services
I. Tests and maintains network infrastructure including software and hardware devices	Basic	Operate and Maintain	Network Services
J. Establishes adequate access controls based on principles of least privilege and need-to-know	Intermediate	Operate and Maintain	Network Services
K. Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines	Basic	Operate and Maintain	Systems Security Analysis

JOB FUNCTION 4: Installs, configures, troubleshoots and maintains server configurations to ensure their confidentiality, integrity and availability; also manages accounts, firewalls, configuration, patch and vulnerability management. Is responsible for access control, security configuration and administration	Core or Optional		Level
Competencies	Level	NICE Framework Category	NICE Framework Specialty Area

A. Checks system hardware availability, functionality, integrity and efficiency	Intermediate	Operate and Maintain	System Admin
B. Conducts functional and connectivity testing to ensure continuing operability	Basic	Operate and Maintain	System Admin
C. Conducts periodic server maintenance including cleaning (physically and electronically), disk checks, system configuration and monitoring, data downloads, backups and testing	Basic	Operate and Maintain	System Admin
D. Assists in the development of group policies and access control lists to ensure compatibility with organizational standards, business rules and needs	Advanced	Operate and Maintain	System Admin
E. Documents compliance with or changes to system administration standard operating procedures	Intermediate	Operate and Maintain	System Admin
F. Installs server fixes, updates and enhancements	Intermediate	Operate and Maintain	System Admin
G. Maintains baseline system security according to organizational policies	Intermediate	Operate and Maintain	System Admin
H. Manages accounts, network rights and access to systems and equipment	Basic	Operate and Maintain	System Admin
I. Monitors and maintains server configuration	Intermediate	Operate and Maintain	System Admin
J. Supports network components	Basic	Operate and Maintain	System Admin
K. Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs	Basic	Operate and Maintain	System Admin
L. Verifies data redundancy and system recovery procedures	Intermediate	Operate and Maintain	System Admin

M. Assists in the coordination or installation of new or modified hardware, operating systems and other baseline software	Intermediate	Operate and Maintain	System Admin
N. Provides ongoing optimization and problem-solving support	Intermediate	Operate and Maintain	System Admin
O. Resolves hardware/software interface and interoperability problems	Basic	Operate and Maintain	System Admin
P. Establishes adequate access controls based on principles of least privilege, role based access controls (RBAC) and need-to-know	Advanced	Operate and Maintain	System Admin

JOB FUNCTION 5: Configures tools and technologies to detect, mitigate and prevent potential threats	Core or Optional		Level
Competencies	Level	NICE Framework Category	NICE Framework Specialty Area
A. Installs and maintains cyber security detection, monitoring and threat management software	Intermediate		
B. 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	Intermediate		
C. Manages IP addresses based on current threat environment	Intermediate		
D. Ensures application of security patches for commercial products integrated into system design	Basic		
E. Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity	Advanced		

JOB FUNCTION 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities	Core or Optional	Level

Competencies	Level	NICE Framework Category	NICE Framework Specialty Area
A. Applies security policies to meet security objectives of the system	Intermediate	Operate and Maintain	Systems Security Analysis
B. Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices	Intermediate	Operate and Maintain	Systems Security Analysis
C. Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs	Basic	Operate and Maintain	Systems Security Analysis
D. Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization	Advanced	Operate and Maintain	Systems Security Analysis
E. Installs, manages and updates intrusion detection system	Advanced	Operate and Maintain	Systems Security Analysis
F. Performs technical and non-technical risk and vulnerability assessments of relevant technology focus areas	Advanced	Protect and Defend	Vulnerability Assessment & Management
G. Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results	Intermediate	Protect and Defend	Vulnerability Assessment & Management
H. Documents systems security operations and maintenance activities	Intermediate	Operate and Maintain	Systems Security Analysis
I. Communicates potential risks or vulnerabilities to manager. Collaborates with others to recommend vulnerability corrections	Advanced	Protect and Defend	Computer Network Defense and Analysis
J. 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	Core or Optional		Level
Competencies	Level	NICE Framework Category	NICE Framework Specialty Area
A. Identifies organizational trends with regard to the security posture of systems; identifies unusual patterns or activities	Basic	Operate and Maintain	Systems Security Analysis
B. Characterizes and analyzes network traffic to identify anomalous activity and potential threats; performs computer network defense trend analysis and reporting	Advanced	Protect and Defend	Computer network Defense and Analysis
C. Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts	Advanced	Protect and Defend	Computer network Defense and Analysis
D. Runs tests to detect real or potential threats, viruses, malware, etc.	Advanced		
E. Assists in researching cost-effective security controls to mitigate risks	Intermediate	Protect and Defend	Vulnerability Assessment and Management
F. Helps perform damage assessments in the event of an attack	Advanced		
G. Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities	Advanced	Operate and Maintain	Systems Security Analysis
H. Documents and escalates incidents that may cause immediate or long-term impact to the environment	Intermediate	Protect and Defend	Computer network Defense Analysis
I. Provides timely detection, identification and alerts of possible attacks and intrusions, anomalous activities, and distinguish these incidents and events from normal baseline activities	Advanced	Protect and Defend	Computer network Defense Analysis
J. Uses network monitoring tools to capture and analyze network traffic associated with malicious activity	Advanced	Investigate	Digital Forensics

K. Performs intrusion analysis	Advanced	Investigate	Digital Forensics
L. Sets containment blockers to align with company policy regarding computer use and web access	Intermediate	Protect and Defend	Computer network Defense Analysis

JOB FUNCTION 8: Responds to cyber intrusions and attacks and provides defensive strategies	Core or Optional		Level
Competencies	Level	NICE Framework Category	NICE Framework Specialty Area
A. Assists in the development of appropriate courses of action in response to identified anomalous network activity	Advanced	Protect and Defend	Computer network Defense Analysis
B. 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
C. Reconstructs a malicious attack or activity based on network traffic	Advanced	Protect and Defend	Computer network Defense Analysis
D. Correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation	Advanced	Protect and Defend	Incident Response
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	Advanced	Protect and Defend	Incident Response
F. 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
G. Performs computer network defense incident triage to include determining scope, urgency and potential impact; identifies the specific vulnerability; provides training recommendations; and makes	Advanced	Protect and Defend	Incident Response

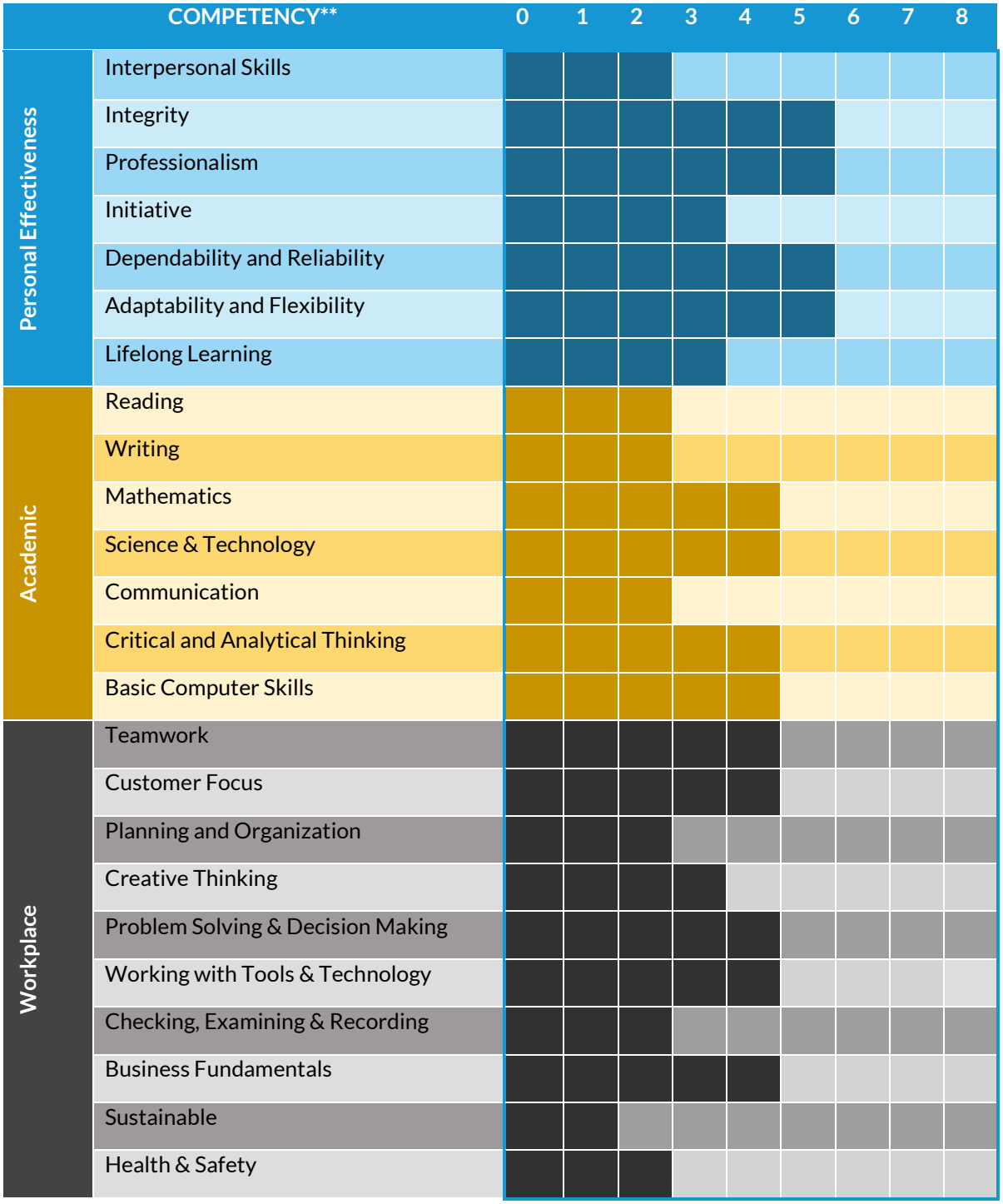
	recommendations that enable expeditious remediation			
H.	Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts	Advanced	Protect and Defend	Incident Response
I.	Tracks and documents computer network defense incidents from initial detection through final resolution	Intermediate	Protect and Defend	Incident Response
J.	Collects intrusion artifacts and uses discovered data to enable mitigation of potential computer network defense (CND) incidents	Advanced	Protect and Defend	Incident Response
K.	Performs virus scanning on digital media	Basic	Investigate	Digital forensics

Related Technical Instruction Plan

COURSE NAME	Course Number
	Hours
LEARNING OBJECTIVES	
COURSE NAME	Course Number
	Hours
LEARNING OBJECTIVES	
COURSE NAME	Course Number
	Hours
LEARNING OBJECTIVES	
COURSE NAME	Course Number
	Hours

LEARNING OBJECTIVES	
COURSE NAME	Course Number
	Hours
LEARNING OBJECTIVES	

Cross-Cutting Competencies



**Cross-cutting competencies are defined in the Competency Model Clearinghouse:

https://www.careeronestop.org/CompetencyModel/competency-models/buidling-blocks-model.aspx

Cross-Cutting Competencies identify transferable skills – sometimes called "soft skills" or "employability skills" – that are important for workplace success, regardless of a person's occupation. Still, the relative importance of specific cross-cutting competencies differs from occupation to occupation. The Cross-Cutting Competencies table, above, provides information about which of these competencies is most important to be successful in a particular occupation. This information can be useful to employers or intermediaries in screening and selecting candidates for apprenticeship programs, or to pre-apprenticeship providers that seek to prepare individuals for successful entry into an apprenticeship program.

The names of the cross-cutting competencies come from the U.S. Department of Labor's Competency Model Clearinghouse and definitions for each can be viewed at: https://www.careeronestop.org/CompetencyModel/competency-models/building-blocks-model.aspx

The scoring system utilized to evaluate the level of competency required in each cross cutting skill aligns with the recommendations of the Lumina Foundation's Connecting Credentials Framework. The framework can be found at: http://connectingcredentials.org/wp-content/uploads/2015/05/ConnectingCredentials-4-29-30.pdf

Detailed Job Functions

JOB FUNCTION 1: Assists in developing security policies and protocols; assists in enforcing company compliance with network security policies and protocols

(Codes in parentheses identify the NICE Framework Knowledge, Skill, Task or Ability code associated with each item)

Related Technical Instruction		
KNOWLEDGE	**SKILLS**	**TOOLS & TECHNOLOGIES**
• 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) • Specific operational impacts of cybersecurity lapses (K0006) • Authentication, authorization and access control methods (K-0007) • Known vulnerabilities from alerts, advisories, errata and bulletins (K0040) • Cybersecurity principles and organizational requirements relevant to confidentiality, integrity, availability, authentication and non-repudiation (K0044) • Enterprise's IT goals and objectives (K0101) • Organization's core business/mission processes (K0146) • Organizational IT use security policies (e.g. account creation,	• 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 (S0006)	• 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

password rules, access control) (K0158) • Personally identifiable information data security standards (K0260) • Payment card industry data security standards (K0261) • Personal health information data security standards (K0262) • 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, procurement and administration (K0194) • Organizational training policies (K0215)		

	Core or Optional	Level
Competency A: Locates (in intranet, employee handbook or within software) organizational policies intended to maintain security and minimize risk and explains their use (T0461)	Core	Basic
Competency B: Competency b: Provides guidance to employees on how to access networks, set passwords, reduce security threats and provide defensive measures associated with searches, software downloads, email, Internet, add-ons, software coding and transferred files (T0192)	Optional	Advanced
Competency C: Ensures that password characteristics are explained and enforced and that updates are required and enforced based on appropriate time intervals	Core	Basic
Competency D: Explains company or organization's policies regarding the storage, use and transfer of sensitive data, including intellectual property and	Core	Intermediate

personally identifiable information. Identifies data life cycle, data storage facilities, technologies and describes business continuity risks (T0458/T0871)		
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
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	Intermediate
Competency G: Develops security compliance policies and protocols for external services (i.e. Cloud service providers, software services, external data centers) (T0136)	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	Intermediate

JOB FUNCTION 2: Provides technical support to users or customers

Related Technical Instruction		
KNOWLEDGE	**SKILLS**	**TOOLS & TECHNOLOGIES**
• First Seven Items from Job Function 1 • Measures or indicators of system performance (K0053) • System administration concepts (K0088) • Industry best practices for service desk (K0237) • Organizational security policies (K0242) • Remote access processes, tools and capabilities related to customer support (K0247) • Personal and sensitive data security standards (K-260-K0262) • Information technology risk management policies, requirements and procedures (K0263) • The organization's information classification program and procedures for information compromise (K0287) • 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)	• Conducting research for client-level problems (S0142) • Identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation (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)	• 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)

	Core or Optional	Level
Competency A: Manages inventory of IT resources (T0496)	Core	Basic
Competency B: Diagnoses and resolves customer-reported system incidents (T0482)	Core	Intermediate
Competency C: Installs and configures hardware, software and peripheral equipment for system users (T0491))	Core	Basic
Competency D: Monitors client-level computer system performance (T0468)	Core	Basic
Competency E: Tests computer system performance (T0502)	Core	Basic
Competency F: Troubleshoots system hardware and software (T0237)	Core	Basic
Competency G: Administers accounts, network rights, and access to systems and equipment(T0494/T0144)	Core	Intermediate
Competency H: Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines (T0136/T0485)	Optional	Advanced

JOB FUNCTION 3: Installs, configures, tests, operates, maintains and manages networks and their firewalls including hardware and software that permit sharing and transmission of information

Related Technical Instruction		
KNOWLEDGE	**SKILLS**	**TOOLS & TECHNOLOGIES**
• Knowledge items 1-6, Job Function 1 • 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, transmission 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) • IT 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 (K0053) • Traffic 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 [ITIL]) (K0061) • Remote access technology concepts (K0071) • IT supply chain security and risk management policies, requirements and procedures (K0169) • Network security architecture concepts including topology, protocols, components and principles (K0179) • Windows/Unix ports and services (K0179) • 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	• Analyzing network traffic capacity and performance characteristics (S0004) • Establishing a routing scheme (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 infrastructure contingency and recovery plans (S0150) • Applying cybersecurity methods, such as firewalls, demilitarized	• Network tools • Hubs, switches, routers, bridges, servers, transmission media • Electronic communication systems • Bluetooth, RFID, IR, Wi-Fi, paging, cellular and satellite dishes

(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) • Transmission records (e.g. Bluetooth, Radio Frequency Identification, Infrared Networking, Wireless Fidelity, paging, cellular, satellite dishes) and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly (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 management (K0327) • 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)	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) (A0058)	

	Core or Optional	Level
Competency A: Collaborates with system developers and users to assist in the selection of appropriate design solutions to ensure the compatibility of system component (T0200/T0201)	Optional	Advanced
Competency B: Installs, replaces, configures and optimizes network hubs, routers and switches (T0035/T0126)	Optional	Advanced

Competency C: Assists in network backup and recovery procedures (T0065)	Opt	Advanced
Competency D: Diagnoses network connectivity problems (T0081)	Opt	Advanced
Competency E: Modifies network infrastructure to serve new purposes or improve workflow	Opt	Advanced
Competency F: Integrates new systems into existing network architecture (T0121/T0129)	Opt	Advanced
Competency G: Patches network vulnerabilities to ensure information is safeguarded against outside parties (T0125/T0160)	Opt	Advanced
Competency H: Repairs networks connectivity problems (T0081)	Opt	Advanced
Competency I: Tests and maintains network infrastructure including software and hardware devices (T0153/T0232)	Core	Intermediate
Competency J: Establishes adequate access controls based on principles of least privilege and need-to-know (T0475)	Core	Advanced
Competency K: Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines (T0461)	Core	Basic

JOB FUNCTION 4: Installs, configures, troubleshoots and maintains server configurations to ensure their confidentiality, integrity and availability; also manages accounts, firewalls, configuration, patch and vulnerability management. Is responsible for access control, security configuration and administration

Related Technical Instruction		
KNOWLEDGE	**SKILLS**	**TOOLS & TECHNOLOGIES**
• Host/network access control mechanisms (access control list) (K0033) • Known vulnerabilities from alerts, advisories, errata and bulletins (K0040) • IT architectural concepts and frameworks (K0047) • IT security principles and methods (e.g. firewalls, demilitarized zones, encryption) (K0049) • Measures or indicators of system performance (K0053) • Network access, identity and access management (K0056) • Performance tuning tools and techniques (K0064) • Policy-based and risk-adaptive access controls (K0065) • Capabilities and functionality associated with various technologies for organizing and managing information (K0095) • Capabilities and functionality of collaborative technologies (K0096) • Server and client operating systems (K0077) • Server diagnostic tools and fault identification techniques (K0078) • Systems administration concepts (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]) (K0117) • Organizational information technology user security policies (e.g. account	• Configuring and optimizing software (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) • Interfacing with customers (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)	• Servers • Desktop/laptop computers • Personal Communication Devices • Diagnostic tools and software • Database software • Networking tools

creation password rules, access control) (K0158) • Basic system administration, network and operating system hardening techniques (K0167) • Network security architecture concepts including topology, protocols, components, and principles (K0169) • Transmission records and jamming techniques that enable transmission of undesirable information or prevent installed systems from operating correctly (K0181) • Data classification standards and methodologies based on sensitivity and other risk factors (K0195) • Data backup and restoration concepts (K0210) • Confidentiality, integrity and availability requirements (K0211) • Personally Identifiable Data (PID) security standards (K0260) • Payment Card Industry data security standards (K0261) • Personal Health Information (PHI) data security standards (K0262) • Systems engineering theories, concepts and methods) K0280) • Developing and applying user credential management system (K0284) • Organization's information classification program and procedures for information compromise (K0287) • System/server diagnostic tools and fault identification techniques (K0289) • Operating system command line/prompt (K0318)	• Operating system administration (S0158)	

	Core or Optional	Level
Competency A: Checks system hardware availability, functionality, integrity and efficiency (T0431)	Core	Intermediate
Competency B: Conducts functional and connectivity testing to ensure continuing operability (T0029)	Core	Basic

Competency C: Conducts periodic server maintenance including cleaning (physically and electronically), disk checks, system configuration and monitoring, data downloads, backups and testing (T0435)	Core	Basic
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	Advanced
Competency E: Documents compliance with or changes to system administration standard operating procedures (T0063)	Core	Intermediate
Competency F: Installs server fixes, updates and enhancements (T0418)	Core	Intermediate
Competency G: Maintains baseline system security according to organizational policies (T0136)	Core	Intermediate
Competency H: Manages accounts, network rights and access to systems and equipment (T0144)	Core	Basic
Competency I: Monitors and maintains server configuration (T0498/T0501)	Core	Intermediate
Competency J: Supports network components	Core	Basic
Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs (T0514/T0515)	Core	Basic
Competency L: Verifies data redundancy and system recovery procedures (T0186)	Core	Basic
Competency M: Assists in the coordination or installation of new or modified hardware,	Core	Intermediate

operating systems and other baseline software (T0507)		
Competency N: Provides ongoing optimization and problem-solving support (T0207)	Core	Intermediate
Competency O: Resolves hardware/software interface and interoperability problems (T0531)	Core	Basic
Competency P: Establishes adequate access controls based on principles of least privilege, role based access controls (RBAC) and need-to-know (T0475)	Opt	Advanced

JOB FUNCTION 5: Configures tools and technologies to detect, mitigate and prevent potential threats

Related Technical Instruction		
KNOWLEDGE	**SKILLS**	**TOOLS & TECHNOLOGIES**
• Knowledge of application vulnerabilities (K0009) • Knowledge of data backups, types of backups and recovery concept tools (K0021) • Host/network access control mechanisms (K0033) • Cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation) (K0044) • Virtual private network security (K0104) • Web filtering technologies (K0135) • Cyberdefense policies, procedures and regulations (K0157) • Current and emerging cyber technology (K02335) • Intrusion detection systems, intrusion prevention system tools and applications (K0324)	• Host/network access control mechanisms (e.g. access control list) (S0007) • Virtual private network security (S0059) • Securing network communication (S0077) • Protecting a network against malware (S0079) • System, network and OS hardening techniques (S0121) • Troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution (S0124)	• Networking tools and software • Intrusion detection software • Virtual Private Network technologies • Web filtering technologies • Servers and back-up systems

	Core or Optional	Level
Competency A: Installs and maintains cyber security detection, monitoring and threat management software (T0485)	Core	Intermediate
Competency B: 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 (T0042)	Core	Intermediate

Competency C: Manages IP addresses based on current threat environment (T0042)	Core	Intermediate
Competency D: Ensures application of security patches for commercial products integrated into system design (T0554)	Core	Basic
Competency E: Uses computer network defense tools for continual monitoring and analysis of system activity to identify malicious activity (T0023)	Optional	Advanced

JOB FUNCTION 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities

Related Technical Instruction		
KNOWLEDGE	**SKILLS**	**TOOLS & TECHNOLOGIES**
• Hacking methodologies in Windows or Unix/Linus environment (K011) • 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 (K0343)	• 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)	• Penetration tools • Authentication devices • Windows/Unix/Linux operating systems • Network traffic monitoring tools • Servers • Backup systems

	Core or Optional	Level
Competency A: Applies security policies to meeting security objectives of the system (T0016/T0438)	Core	Intermediate
Competency B: Performs system administration to ensure current defense applications are in place,	Core	Intermediate

including on Virtual Private Network devices (T0180/T0086)		
Competency C: Ensures that data back up and restoration systems are functional and consistent with company's document retention policy and business continuity needs (T0186/T0050)	Core	Basic
Competency D: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization (T0502)	Optional	Advanced
Competency E: Installs, manages and updates intrusion detection system (T0309)	Optional	Advanced
Competency F: Performs technical and non-technical risk and vulnerability assessments of relevant technology focus areas (T0549/T0178)	Optional	Advanced
Competency G: Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results (T0051/T0252)	Core	Intermediate
Competency H: Documents systems security operations and maintenance activities (T0470)	Core	Intermediate
Competency I: Communicates potential risks or vulnerabilities to manager. Collaborates with others to recommend vulnerability corrections (T0178)	Optional	Advanced
Competency J: Identifies information technology security program implications of new technologies or technology upgrades (T0115)	Optional	Advanced

JOB FUNCTION 7: Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats

Related Technical Instruction		
KNOWLEDGE	**SKILLS**	**TOOLS & TECHNOLOGIES**
• Application vulnerabilities (K0009) • Data backups, types of backups and recovery concepts and tools (K0021) • Disaster recovery continuity of operations plans (K0026) • Host access control mechanisms (k0033) • Incident categories, incident 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 (K0066) • Incident response and handling methodologies (K0042)	• Conducting vulnerability scans (S0001) • Identifying, capturing and containing malware (S0003) • Applying host/network access controls (S0007) • Applying security models (S0139) • 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)	• Data backup tools and technologies • Networking devices • Network traffic detection devices • Intrusion detection technologies • Software/Applications of relevance to organization • Malware

	Core or Optional	Level
Competency A: Identifies organizational trends with regard to the security posture of systems; identifies unusual patterns or activities (T019)	Core	Basic
Competency B: Characterizes and analyzes network traffic to identify anomalous activity and	Optional	Advanced

potential threats; performs computer network defense trend analysis and reporting (T0333)		
Competency C: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts (T00434/T0214)	Optional	Advanced
Competency D: Runs tests to detect real or potential threats, viruses, malware, etc. (T2096/T2097)	Optional	Advanced
Competency E: Assists in researching cost-effective security controls to mitigate risks (T0550/T0310)	Core	Intermediate
Competency F: Helps perform damage assessments in the event of an attack	Optional	Advanced
Competency G: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities (T0164)	Optional	Advanced
Competency H: Documents and escalates incidents that may cause immediate or long-term impact to the organization or environment (T0155)	Core	Intermediate
Competency I: Provides timely detection, identification and alerts of possible attacks and intrusions, anomalous activities, and distinguishes these incidents and events from normal baseline activity (T0258/T0214)	Optional	Advanced
Competency J: Uses network monitoring tools to capture and analyze network traffic associated with malicious activity (T0259)	Optional	Advanced
Competency K: Performs intrusion analysis (T0169)	Optional	Advanced

Competency L: Sets containment blockers to align with company policy regarding computer use and web access (T0494)	Optional	Advanced

JOB FUNCTION 8: Responds to cyber intrusions and attacks and provides defensive strategies

Related Technical Instruction		
KNOWLEDGE	**SKILLS**	**TOOLS & TECHNOLOGIES**
• Concepts and practices for processing digital forensic data (K0017) • Data backups, types of backups and recovery concepts and tools (K0021) • Incident response and handling methodologies (K0042) • Operating systems (K0060) • Server diagnostic tools and fault identification techniques (K0078) • Process for seizing and preserving digital evidence (e.g. chain of custody) (K0118) • Web mail collection, searching/analyzing techniques, tools and cookies (K0131) • System files (log files, registry files, configuration files) contain relevant information and where to find those system files (K0132) • Types of digital forensics data and how to recognize them (K0133) • Virtual machine aware malware, debugger aware malware and packing (K0199) • System and application security threats and vulnerabilities **(K0070)**	• Troubleshooting failed system components (T0150) • Developing, testing and implementing network infrastructure contingency and recovery plans (S0032) • Packet-level analysis using appropriate tools (e.g. wireshart, tcpdump) (S0046) • Preserving evidence integrity according to standard operating procedures or national standards (S0047) • Analyzing memory dumps to extract information (S0062) • Identifying, modifying and manipulation applicable system components within Windows, Unix or Linus (e.g. passwords, user accounts, files) (S0067) • Using forensic tools suites (e.g. EnCase, Sleuthkit, FTK) (S0071) • Physically disassembling PCs (S0074)	• Wireshark Tcpdump • EnCase, Sleuthkit, FTK • Virtual machines • Security event correlation tools • Forensic tools such as Wireshark and VMWare • Malware analysis tools (Oily Debug, Ida Pro)

	Core or Optional	Level
Competency A: Assists in the development of appropriate courses of action in response to identified anomalous network activity (T0295)	Optional	Advanced
Competency B: Triages systems operations impact: malware, worms, man-in-the-middle attack, denial of service, rootkits, keystroke loggers, SQL injection and cross-site scripting (T0504)	Optional	Advanced
Competency C: Reconstructs a malicious attack or activity based on network traffic (T0298)	Optional	Advanced
Competency D: Correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation (T0260/T0292)	Optional	Advanced
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 (T0166/T0167)	Optional	Advanced
Competency F: Performs analysis of log files from a variety of sources to identify threats to network security; performs file signature analysis (T0433/T0167)	Optional	Advanced
Competency G: Performs analysis of log files from a variety of sources to identify threats to network security; performs file signature analysis (T0433/T0167)	Optional	Advanced
Competency H: Receives and analyzes network alerts from various sources within the enterprise	Optional	Advanced

and determines possible causes of such alerts (T0293)		
Competency I: Tracks and documents computer network defense incidents from initial detection through final resolution (T0395/T0232)	Core	Intermediate
Competency J: Collects intrusion artifacts and uses discovered data to enable mitigation of potential computer network defense (CND) incidents (T0278)	Optional	Advanced
Competency K: Performs virus scanning on digital media	Core	Basic

URBAN
INSTITUTE · ELEVATE · THE · DEBATE

2100 M Street NW
Washington, DC 20037

www.urban.org