Occupation: Cyber Security Support Technician	**ONET Code 15-1122**
	RAPIDS Code

OCCUPATIONAL OVERVIEW

Potential Job Titles: Cyber security analyst, cyber security monitor, vulnerability analyst, information systems security analyst, network security analyst

Occupational Context: 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.

Occupational Purpose: 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.

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.

Attitudes & 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.

Certification or Licensure:	Accrediting Organizations: Multiple software and hardware vendors offer certification opportunities to demonstrate a wide range of competencies and that enable an individual to continue expanding their knowledge and skills throughout their career. Among those vendors and organizations well known to provide certification opportunities are: CompTIA, Cisco, Microsoft, (ISC)2.
CompTia Security+ (Certification) Certified Information Systems Security Professional (CISSP) (Certification)	

Large Employers	Trade Associations	Regulatory Agencies Department of Homeland Security National Institute of Standards and Technology Department of Defense Department of Treasury Federal Bureau of Investigation

Number of current employees (2014-2024): 85,000

Number of additional job openings predicted (2014-2024): 25,500

Median Salary (2014): $67,375 (depending upon years of experience and industry certifications)

Job Function 1: Assists in developing security policies and protocols: assists in enforcing company compliance with network security policies and protocols		
Job Function 2: Provides technical support to users or customers		
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		
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		
Job Function 5: Configures tools and technologies to detect, mitigate and prevent potential threats		
Job Function 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities		
Job Function 7: Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats		
Job Function 8: Responds to cyber intrusions and attacks and provides defensive strategies		

CROSS-CUTTING COMPETENCIES (These come from the Competency Model Clearinghouse)										
Personal Effectiveness Competencies										
	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				
Academic 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				
	Basic Computer Skills					X				
Workplace Competencies										
	Relevance (Based on Lumina Beta Credentials Framework)	0	1	2	3	4	5	6	7	8
	Teamwork					X				
	Customer Focus					X				
	Planning & Organization			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 **Support Technician**	**Cyber Security**		ONET Code 15-1122.00 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 including vendor certifications). Certified Information Systems Security Professional (CISSP) is another core certification, but it does require candidates to have 5 years of work experience, so certification may not take place during the apprenticeship program.			

JOB FUNCTION	LEVEL	NICE Framework Category	NICE Framework Specialty Area
JOB FUNCTION 1: Assists in developing security policies and protocols; assists in enforcing company compliance with network security policies and protocols			
Competency 1a: 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
Competency 1b: 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	Advanced	Securely Provision	Information Assurance Compliance
Competency 1c: 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
Competency 1d: 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
Competency 1e: 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
Competency 1f: 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
Competency 1g: 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
Competency 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 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			
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 system users	Basic	Operate and Maintain	Customer service Technical support
Competency 2d: Monitors client-level computer system performance	Basic	Operate and Maintain	Customer service Technical support
Competency 2e: Tests computer system performance	Basic	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	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 and 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 switches	Advanced	Operate and Maintain	Network Services

Competency 3c: Assists in network backup and recovery procedures				Intermediate	Operate and Maintain	Network Services	
Competency 3d: Diagnoses network connectivity problems				Basic	Operate and Maintain	Network Services	
Competency 3e: Modifies network infrastructure to serve new purposes or improve workflow				Advanced	Operate and Maintain	Network Services	
Competency 3f: Integrates new systems into existing network architecture				Intermediate	Operate and Maintain	Network Services	
Competency 3g: Patches network vulnerabilities to ensure information is safeguarded against outside parties				Intermediate	Operate and Maintain	Network Services	
Competency 3h: Repairs network connectivity problems				Basic	Operate and Maintain	Network Services	
Competency 3i: Tests and maintains network infrastructure including software and hardware devices				Basic	Operate and Maintain	Network Services	
Competency 3j: Establishes adequate access controls based on principles of least privilege and need-to-know				Intermediate	Operate and Maintain	Systems Security Analysis	
Competency 3k: Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines				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							
Competency 4a: Checks system hardware availability, functionality, integrity and efficiency				Intermediate	Operate and Maintain	System Admin	
Competency 4b: Conducts functional and connectivity testing to ensure continuing operability				Basic	Operate and Maintain	System Admin	
Competency 4c: 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	
Competency 4d: 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	
Competency 4e: Documents compliance with or changes to system administration standard operating procedures				Intermediate	Operate and Maintain	System Admin	
Competency 4f: Installs server fixes, updates and enhancements				Intermediate	Operate and Maintain	System Admin	
Competency 4g: Maintains baseline system security according to organizational policies				Intermediate	Operate and Maintain	System Admin	
Competency 4h: Manages accounts, network rights and access to systems and equipment				Basic	Operate and Maintain	System Admin	
Competency 4i: Monitors and maintains server configuration				Intermediate	Operate and Maintain	System Admin	
Competency 4j: Supports network components				Basic	Operate and Maintain	System Admin	
Competency 4k: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs				Basic	Operate and Maintain	System Admin	
Competency 4l: Verifies data redundancy and system recovery procedures				Intermediate	Operate and Maintain	System Admin	
Competency 4m: Assists in the coordination or installation of new or modified hardware, operating systems and other baseline software				Intermediate	Operate and Maintain	System Admin	
Competency 4n: Provides ongoing optimization and problem-solving support				Intermediate	Operate and Maintain	System Admin	
Competency 4o: Resolves hardware/software interface and interoperability problems				Basic	Operate and Maintain	System Admin	
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	Systems Security Analysis	
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				Intermediate	Protect and Defend	Computer Network Defense 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				Intermediate	Protect and Defend	Computer Network Defense Analysis	
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				Basic	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				Advanced	Protect and Defend	Computer Network Defense Analysis	
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				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				Intermediate	Operate and Maintain	Systems Security Analysis	
Competency 6c: 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	
Competency 6d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization				Advanced	Operate and Maintain	Systems Security Analysis	

Competency 6e: Installs, manages and updates intrusion 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 Management	
Competency 6g: Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results				Intermediate	Protect and Defend	Vulnerability Assessment and Management	
Competency 6h: Documents systems security operations and maintenance activities				Intermediate	Operate and Maintain	Systems Security Analysis	
Competency6i: Communicates potential risks or vulnerabilities to manager. Collaborates with others to recommend vulnerability corrections				Advanced	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				Basic	Operate and Maintain	Systems Security Analysis	
Competency 7b: 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	
Competency 7c: 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	
Competency 7d: Runs tests to detect real or potential threats, viruses, malware, etc.				Advanced			
Competency 7e: Assists in researching cost-effective security controls to mitigate risks				Intermediate	Protect and Defend	Vulnerability Assessment and	
Competency 7f: Helps perform damage assessments in the event of an attack				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				Advanced	Protect and Defend	Computer network Defense Analysis	
Competency 7j: Uses network monitoring tools to capture and analyze network traffic associated with malicious activity				Advanced	Investigate	Digital Forensics	
Competency 7k: Performs intrusion analysis				Advanced	Investigate	Digital Forensics	
Competency 7l: 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							
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 Response	
Competency 8k: Performs virus scanning on digital media				Basic	Investigate	Digital forensics	

Job Function 1: Assists in developing security policies and protocols; assists in enforcing company compliance with network security policies and protocols			
RELATED INSTRUCTION	NICE Framework	Core/Optional	LEVEL
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	S0006		
Knowledge & Understanding			
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	K0007		
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, password rules, access control)	K0158		
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, procurement and administration	K0194		
Organizational traning policies	K0215		
Tools & 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			
COMPETENCIES			
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
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 security threats and provide defensive measures associated with searches, software downloads, email, Internet, add-ons, software coding and transferred files	T0192	Optional	Advanced
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			
	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	Intermediate
	Performance Standards			
	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			
	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
	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			
	Competency h: Complies with incident response and handling methodologies	T0331	Optional	Advanced
	Performance Standards			

	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
	Performance Standards			

Job Function 2: Provides technical support to users or customers			
RELATED INSTRUCTION	NICE Framework	Core/Optional	LEVEL
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		
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	K0260-K0262		
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		
COMPETENCIES			
Competency a: Manages inventory of IT resources	T0496	Core	Basic
Performance Standards			
Competency b: Diagnoses and resolves customer-reported system incidents	T0482	Core	Intermediate
Performance Standards			

	Competency c: Installs and configures hardware, software and peripheral equipment for system users	T0491	Core	Basic
	Performance 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			
	Competency g: Administers accounts, network rights, and access to systems and equipment	T0494/TO144	Core	Intermediate
	Performance Standards			
	Competency h: Implements security measures for uses in system and ensures that system designs incorporate security configuration guidelines	T0136/T0485	Optional	Advanced
	Performance Standards			

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 INSTRUCTION	NICE Framework	Core/Optional	LEVEL
Skills			
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 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, 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 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		
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		
	Tools & Technologies			
	Network tools			
	Hubs, switches, routers, bridges, servers, transmission media			
	Electronic communication systems			
	Bluetooth, RFID, IR, Wi-Fi, paging, cellular and satellite dishes			
COMPETENCIES				
	Competency a: Collaborates with system developers and users to assist in the selection of appropriate design solutions to ensure the compatibility of system components	T0200/T0201	Optional	Advanced
	Performance Standards			
	Competency b: Installs, replaces, configures and optimizes network hubs, routers and switches	T0035/T0126	Optional	Advanced
	Performance Standards			
	Competency c: Assists in network backup and recovery procedures	T0065	Optional	Advanced
	Performance Standards			
	Competency d: Diagnoses network connectivity problems	T0081	Optional	Advanced
	Performance Standards			
	Competency e: Modifies network infrastructure to serve new purposes or improve workflow		Optional	Advanced

	Performance Standards			
	Competency f: Integrates new systems into existing network architecture	T0121/T0129	Optional	Advanced
	Performance Standards			
	Competency g: Patches network vulnerabilities to ensure information is safeguarded against outside parties	T0125/T0160	Optional	Advanced
	Performance Standards			
	Competency h: Repairs network connectivity problems	T0081	Optional	Advanced
	Performance Standards			
	Competency i: Tests and maintains network infrastructure including software and hardware devices	T0153/T0232	Core	Intermediate
	Performance Standards			
	Competency j: Establishes adequate access controls based on principles of least privilege and need-to-know	T0475	Core	Advanced
	Performance Standards			
	Competency k: Implements security measures for users in system and ensures that system designs incorporate security configuration guidelines	T0461	Core	Basic

	Performance Standards			

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 INSTRUCTION	NICE Framework	Core/Optional	LEVEL
Skills			
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		
Operating system administration	S0158		
Knowledge & Understanding			
See K0001 - K0006 from job function 1	*K0001-K0006*		
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 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	K0179		
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	Optional	
Personal Health Information (PHI) data security standards	K0262	Optional	
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		

	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	Intermediate
	Performance Standards			
	Competency b: Conducts functional and connectivity testing to ensure continuing operability	T0029	Core	Basic
	Performance Standards			
	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
	Performance Standards			
	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
	Performance Standards			
	Competency e: Documents compliance with or changes to system administration standard operating procedures	T0063	Core	Intermediate
	Performance Standards			

	Competency f: Installs server fixes, updates and enhancements	T0418	Core	Intermediate
	Performance Standards			
	Competency g: Maintains baseline system security according to organizational policies	T0136	Core	Intermediate
	Performance Standards			
	Competency h: Manages accounts, network rights and access to systems and equipment	T0144	Core	Basic
	Performance Standards			
	Competency i: Monitors and maintains server configuration	T0498/T0501	Core	Intermediate
	Performance Standards			
	Competency j: Supports network components		Core	Basic
	Performance Standards			
	Competency K: Diagnoses faulty system/server hardware; seeks appropriate support or assistance to perform server repairs	T0514/T0515	Core	Basic
	Performance Standards			

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

Job Function 5: Configures tools and technologies to detect, mitigate and prevent potential threats			
RELATED INSTRUCTION	NICE Framework	Core/Optional	LEVEL
Skills			
K0001-K0006 from job function 1			
Applying host/network access controls (e.g. access control list)	S0007		
Virtual private network devices and encryption	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		
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			
COMPETENCIES			
Competency a: Installs and maintains cyber security detection, monitoring and threat management software	T0485	Core	Intermediate
Performance Standards			
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
Performance Standards			
Competency c: Manages IP addresses based on current threat environment	T0042	Core	Intermediate
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			

Job function 6: Assesses and mitigates system network, business continuity and related security risks and vulnerabilities			
RELATED INSTRUCTION	NICE Framework	Core/Optional	LEVEL
Skills			
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			
COMPETENCIES			
Competency a: Applies security policies to meet security objectives of the system	T0016/T0438	Core	Intermediate
Performance Standards			
Competency b: Performs system administration to ensure current defense applications are in place, including on Virtual Private Network devices	T0180/T0086	Core	Intermediate
Performance Standards			

	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
	Performance Standards			
	Competency d: Identifies potential conflicts with implementation of any computer network defense tools. Performs tool signature testing and optimization	T0504	Optional	Advanced
	Performance Standards			
	Competency e: Installs, manages and updates intrusion detection system	T0309	Optional	Advanced
	Performance Standards			
	Competency f: Performs technical and non-technical risk and vulnerability assessments of relevant technology focus areas	T0549/T0178	Optional	Advanced
	Performance Standards			
	Competency g: Conducts authorized penetration testing (Wi-Fi, network perimeter, application security, cloud, mobile devices) and assesses results	T0051/T0252	Core	Intermediate
	Performance Standards			
	Competency h: Documents systems security operations and maintenance activities	T0470	Core	Intermediate
	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			

Job Function 7: Reviews network utilization data to identify unusual patterns, suspicious activity or signs of potential threats			
RELATED INSTRUCTION	NICE Framework	Core/Optional	LEVEL
Skills			
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		
Knowledge & Understanding			
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, 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	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			
COMPETENCIES			
Competency a: Identifies organizational trends with regard to the security posture of systems; identifies unusual patterns or activities	T0198	Core	Basic
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	Advanced
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/ T0088/T0503	Core	Intermediate
	Performance Standards			
	Competency f: Helps perform damage assessments in the event of an attack		Optional	Advanced
	Performance Standards			
	Competency g: Monitors network data to identify unusual activity, trends, unauthorized devices or other potential vulnerabilities	T0164	Optional	Advanced
	Performance Standards			
	Competency h: Documents and escalates incidents that may cause immediate or long-term impact to the environment	T0155	Core	Intermediate
	Performance Standards			

	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
	Performance Standards			
	Competency l: Sets containment blockers to align with company policy regarding computer use and web access	T0494	Core	Intermediate
	Performance Standards			

Job Function 8: Responds to cyber intrusions and attacks and provides defensive strategies				
	RELATED INSTRUCTION	NICE Framework	Core/Optional	LEVEL
	Skills			
	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 manipulationg 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		
	Knowledge & Understanding			
	K0001-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		
	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 informaiton 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		
	Tools & Technologies			
	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)			
COMPETENCIES				
O	Competency a: Assists in the development of appropriate courses of action in response to identified anomalous network activity	T0295	Optional	Advanced
	Performance Standards			
O	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
	Performance Standards			
O	Competency c: Reconstructs a malicious attack or activity based on network traffic	T0298	Optional	Advanced
	Performance Standards			

O	Competency d: Correlates incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation	T0260/T0292	Optional	Advanced
	Performance Standards			
O	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
	Performance Standards			
O	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
	Performance Standards			
O	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	T0047	Optional	Advanced
	Performance Standards			
O	Competency h: Receives and analyzes network alerts from various sources within the enterprise and determines possible causes of such alerts	T0293	Optional	Advanced
	Performance Standards			

C	Competency i: Tracks and documents computer network defense incidents from initial detection through final resolution	T0395/T0233/	Core	Intermediate
	Performance Standards			
O	Competency j: Collects intrusion artifacts and uses discovered data to enable mitigation of potential computer network defense (CND) incidents	T0278	Optional	Advanced
	Performance Standards			
C	Competency k: Performs virus scanning on digital media		Core	Basic
	Performance Standards			

	Job Function 6: Review network utilization data to identify unusual patterns, suspicious activity or signs of potential threats	LEVEL	OJT	RI
	Scope			
	Skills			
	Developing and deploying signatures	S0020		
	Incident handling methodologies	S0054		
	Using protocol analyzers	S0057		
	Recognizing and categorizing types of vulnerabilities and associated attacks	S0078		
	Reading and interpreting signatures	S0096		
	Assessing security controls based on cybersecurity principles and tenents	S0147		
	Recognizing vulnerabilities in security systems	S0167		
	Conducting trend analysis	S0169		
	Knowledge & Understanding			
	Cyber defense and vulnerability assessment tools, including open source tools, and their capabilities	K0013		
	Host/network access control mechanisms	*K0033*		
	Cybersecurity principles used to manage risks related to the use, processing, storage and transmission of information or data	K0038		
	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 intrusion detection technologies	K0046		
	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	K0190		
	Countermeasure design for identified security risks	K0298		
	Different classes of attacks (e.g. passive, active, insider, close-in, distribution)	K0161		
	Tools & Technologies			
Core or Optional	Competency a: Identify organizational trends with regard to the security posture of systems; identify unusual patterns or activities	T0469/T0470		
	Performance Standards			
Core or Optional	Competency b: Characterize and analyze network traffic to identify anomalous activity and potential threats; perform computer network defense trend analysis and reporting	T0333		
	Performance Standards			

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		
	Performance Standards			
Core or Optional	Competency e: Assists in researching cost-effective security controls to mitigate risks	T0310/T0550		
	Performance Standards			
Core or Optional	Competency f: Perform damage assessments in the event of an attack			
	Performance Standards			
Core or Optional	Competency g:			
	Performance Standards			
Core or Optional	Competency h:			
	Performance Standards			

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

Job Function :		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 Optional	Competency g:			
	Performance Standards			
Core or Optional	Competency h:			
	Performance Standards			
Core or Optional	Competency i:			
	Performance Standards			

Core or Optional	Competency j:			
	Performance Standards			

Job Function :		LEVEL	OJT	RI
	Scope			
	Skills			
	Knowledge & Understanding			
	Certifications			
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 Optional	Competency g:			
	Performance Standards			
Core or Optional	Competency h:			
	Performance Standards			
Core or Optional	Competency i:			
	Performance Standards			

Core or Optional	Competency j:			
	Performance Standards			

Job Function :		LEVEL	OJT	RI
	Scope			
	Skills			
	Knowledge & Understanding			
	Toos & 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 Optional	Competency g:			
	Performance Standards			
Core or Optional	Competency h:			
	Performance Standards			
Core or Optional	Competency i:			
	Performance Standards			

Core or Optional	Competency j:			
	Performance Standards			

Job Function :		LEVEL	OJT	RI
	Scope			
	Skills			
	Knowledge & Understanding			
	Tools & 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 Optional	Competency g:			
	Performance Standards			
Core or Optional	Competency h:			
	Performance Standards			
Core or Optional	Competency i:			
	Performance Standards			

Core or Optional	Competency j:			
	Performance Standards			