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