Office of Apprenticeship
U.S. Department of Labor

Work Process Schedule

Security Support Technician	
Job Description: Install, network, configure, and technically support the ongoing maintenance of electronic security equipment and/or low-voltage technology devices. Assess system vulnerabilities for security risks and implement preventive cybersecurity measures to protect against unauthorized access or malicious attacks/intrusions. Safeguard vital electronic infrastructure and implement risk mitigation strategies to ensure the integrity of technology systems, networks, and devices.	
RAPIDS Code: 2050CB	**O*NET Code:** 15.1212.00
Estimated Program Length: 1 year	
Apprenticeship Type: ☒ Competency-Based ☐ Time-Based ☐ Hybrid	

Suggested On-the-Job Learning Outline

Basic Hardware and IT Security Principles	
Competencies	**Level**
A. Assess the security posture and status of an operational environment.	Intermediate
B. Identify relevant technology and security partners within the broader enterprise environment.	Basic
C. Demonstrate knowledge of common computer hardware, interfaces, and operating systems.	Basic
D. Demonstrate skills required to manage and troubleshoot computer hardware and peripheral devices.	Basic
E. Demonstrate skills required to configure peripheral devices and related applications to support external hardware.	Intermediate
F. Demonstrate knowledge of basic enterprise security concepts and wireless security protocols.	Basic
G. Demonstrate skills required to troubleshoot common computer and application security issues.	Intermediate
H. Demonstrate skills required to troubleshoot wireless connectivity issues.	Intermediate
I. Demonstrate skills required to implement identity and account management controls, including public key infrastructure.	Advanced
J. Demonstrate knowledge of basic networking concepts (wired and wireless).	Basic
K. Demonstrate skills required to configure and troubleshoot device connectivity (LAN and Internet Access).	Basic

Network Security and Troubleshooting	
Competencies	**Level**
A. Demonstrate knowledge of network topologies and network types.	Basic
B. Demonstrate knowledge of cables, types of connectors, and the purpose for each.	Basic
C. Demonstrate skills required to configure a subnet and use appropriate IP addressing schemes.	Intermediate
D. Demonstrate knowledge of ports, protocols, and services, as well as their purpose.	Intermediate
E. Demonstrate knowledge of basic architecture concepts related to corporate and datacenter network environments.	Intermediate
F. Demonstrate knowledge of network devices, their features, and placement within a network.	Basic
G. Demonstrate skills required to configure and deploy Ethernet switching solutions, including VLANs.	Intermediate/Advanced
H. Demonstrate skills required to deploy wireless standards configurations and technologies.	Intermediate
I. Demonstrate skills and best practices required to troubleshoot networking issues.	Intermediate
J. Demonstrate skills required to use network software tools and commands.	Basic
K. Monitor and secure digital information, hybrid physical environments, as well as cloud, mobile, and IoT assessments.	Intermediate

Threats, Attacks, and Vulnerabilities	
Competencies	**Level**
A. Demonstrate knowledge about emerging threats, vulnerabilities, or attack vectors.	Intermediate
B. Demonstrate skills required to analyze potential signs related to application attacks, including network-based attacks.	Intermediate
C. Demonstrate knowledge of types of social engineering methods.	Basic
D. Demonstrate knowledge of types of network attacks.	Basic
E. Maintain current knowledge about emerging system, industry or technology trends, and security threats.	Basic
F. Identify, analyze, and decide appropriate incident response steps and coordinate with appropriate parties.	Advanced

Governance, Risk, and Compliance	
Competencies	**Level**
A. Operate with an awareness of applicable laws, policies, standards, and best practices.	Basic
B. Implement security measures for technology systems to bring projects, sites, or systems into compliance with relevant standards, policies, procedures, or best practices.	Advanced
C. Discover security priorities, policies, procedures, and best practices relevant to a project, site, and systems.	Intermediate
D. Demonstrate knowledge of risk management processes and concepts.	Intermediate
E. Demonstrate knowledge of privacy and sensitive data concepts as they relate to security.	Basic
F. Summarize, report and present non-compliant attributes of a project, site, or system.	Intermediate
G. Recommend, collaborate, and negotiate with others to resolve operational technology security risk to prevent loss or damage.	Advanced

Device Installation	
Competencies	**Level**
A. Ability to install and configure devices, and equipment that operate primarily on the basis of electrical or electronic (not mechanical) principles.	Basic
B. Ability to install, maintain, or repair security systems, electronic devices, or related equipment, following blueprints of electrical layouts and building plans.	Basic
C. Ability to mount and fasten control panels, door and window contacts, sensors, or video cameras, and attach electrical and telephone wiring to connect components.	Basic
D. Ability to feed cables through access holes, roof spaces, or cavity walls to reach fixture outlets, positioning and terminating cables, wires, or strapping.	Basic
E. Ability to drill holes for wiring in wall studs, joists, ceilings, or floors.	Basic
F. Ability to mount raceways and conduits and fasten wires to wood framing, using staplers.	Basic
G. Ability to read and interpret work orders, building plans, and installation manuals to determine materials requirements and installation procedures.	Intermediate

System Integration and Testing	
Competencies	**Level**
A. Demonstrate knowledge of system integration with other systems (hardware or software) in a security solution.	Intermediate/Advanced
B. Demonstrate knowledge of the components, products, and technologies of power requirements for security systems.	Basic
C. Ability to test and repair circuits and sensors, following wiring and system specifications.	Basic
D. Ability to examine security systems to identify/locate problems, determine cause(s) of operating errors and decide what to do about it.	Intermediate
E. Ability to conduct test and troubleshoot security devices, systems, or other product features to ensure proper functioning or to diagnose malfunctions.	Intermediate
F. Demonstrate knowledge of how electrical and power requirements are applied to the components of a security solution.	Basic
G. Demonstrate knowledge of the common incompatibilities, pitfalls, and limitations in security systems.	Intermediate
H. Demonstrate knowledge of how IT/network/cybersecurity integrates with the security solution.	Basic
I. Test and analyze system vulnerabilities to ensure secure functionality.	Advanced

Employability Skills	
Competencies	**Level**
A. Demonstrate skills to provide competent customer service using active listening and empathy during various interactions (e.g., in-person, over telephone, email, and chat).	Basic
B. Demonstrate skills required to problem-solve using critical thinking, clarifying questions, and knowing when to escalate a situation to a superior.	Basic
C. Demonstrate ability to conduct oneself with integrity, professionalism, and in accordance with organization policy and procedure.	Basic
D. Demonstrate skills to communicate with colleagues, managers, and end users effectively and clearly, in a timely manner.	Basic
E. Demonstrate ability to use respectful cross-cultural communication to work successfully across the organization and with diverse coworkers.	Basic

F. Demonstrate knowledge required to manage time effectively, minimizing distractions to maintain productivity, prioritize work appropriately, and meet deadlines with situational awareness.	Basic
G. Demonstrate skills required to take and give productive critical feedback.	Basic
H. Demonstrate skills to explain complex issues to non-technical customers without jargon or blaming.	Intermediate
I. Demonstrate ability to manage stress and other emotions in the workplace to reduce conflict, foster collaboration, and promote wellness.	Basic

Suggested Related Instruction Outline

Provider	
Name: Security Industry Association	
Address: 8455 Colesville Rd. Ste 1200, Silver Spring, MD 20910	
Email: education@securityindustry.org	**Phone Number:** 301-804-4700
Suggested Related Instruction Hours: 144	

Related Instruction Descriptions	Contact Hours
Computer Hardware and Information Technology	8
Cybersecurity and Information Security	36
Device Configuration and System Installation	20
Governance, Risk and Compliance	4
Network Security for Physical Security Devices	36
Security Product Technologies	24
Security Project Management	16
Total	**144**

*Completion of Apprenticeship Program qualifies for one-year (2,000 hours) towards one-the-job experience requirement for Certified Security Project Manager (CSPM) and Security Industry Cybersecurity Certification (SICC).

*Optional certificate or certifications may be available for successful completion of training.