CSX™
CYBERSECURITY NEXUS

CYBERSECURITY FUNDAMENTALS KNOWLEDGE STATEMENTS

DOMAIN 1: CYBERSECURITY CONCEPTS

1.1 Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage and transmission of information or data.

1.2 Knowledge of security management.

1.3 Knowledge of risk management processes, including steps and methods for assessing risk.

1.4 Knowledge of threat actors (e.g., script kiddies, non-nation state sponsored and nation state sponsored).

1.5 Knowledge of cybersecurity roles.

1.6 Knowledge of common adversary tactics, techniques and procedures (TTPs).

1.7 Knowledge of relevant laws, policies, procedures and governance requirements.

1.8 Knowledge of cybersecurity controls.

DOMAIN 2: CYBERSECURITY ARCHITECTURE PRINCIPLES

2.1 Knowledge of network design processes, to include understanding of security objectives, operational objectives and tradeoffs.

2.2 Knowledge of security system design methods, tools and techniques.

2.3 Knowledge of network access, identity and access management.

2.4 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).

2.5 Knowledge of network security architecture concepts, including topology, protocols, components and principles (e.g., application of defense in depth).

2.6 Knowledge of malware analysis concepts and methodology.

2.7 Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies.

2.8 Knowledge of defense in depth principles and network security architecture.

2.9 Knowledge of encryption algorithms (e.g., internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE]).

2.10 Knowledge of cryptography.

2.11 Knowledge of encryption methodologies.

2.12 Knowledge of how traffic flows across the network (i.e. transmission and encapsulation)

2.13 Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS]).

DOMAIN 3: SECURITY OF NETWORKS, SYSTEMS, APPLICATIONS AND DATA

3.1 Knowledge of vulnerability assessment tools, including open source tools, and their capabilities.

3.2 Knowledge of basic system administration, network and operating system hardening techniques.

3.3 Knowledge of risk associated with virtualizations.

3.4 Knowledge of penetration testing.

3.5 Knowledge of network systems management principles, models, methods (e.g., end-to- end systems performance monitoring) and tools.

3.6 Knowledge of remote access technology.

3.7 Knowledge of Unix command line.

3.8 Knowledge of system and application security threats and vulnerabilities.

3.9 Knowledge of system life cycle management principles, including software security and usability.

3.10 Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance and reliability.

3.11 Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, cover channel, replay, return- oriented attacks, malicious code).

3.12 Knowledge of social dynamics of computer attackers in a global context.

3.13 Knowledge of secure configuration management techniques.

3.14 Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media and related hardware.

3.15 Knowledge of communication methods, principles and concepts that support the network infrastructure.

3.16 Knowledge of the common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, email, Domain Name System [DNS]) and how they interact to provide network communications.

3.17 Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Network [WLAN], Wireless Wide Area Network [WWAN]).

3.18 Knowledge of virtualization technologies and virtual machine development and maintenance.

3.19 Knowledge of application security (e.g. SDLC, vulnerabilities, best practices)

3.20 Knowledge of risk threat assessment.

DOMAIN 4: INCIDENT RESPONSE

4.1 Knowledge of incident categories and response.

4.2 Knowledge of business continuity/disaster recovery.

4.3 Knowledge of incident response and handling methodologies.

4.4 Knowledge of security event correlation tools.

4.5 Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody).

4.6 Knowledge of types of digital forensics data.

4.7 Knowledge of basic concepts and practices of processing digital forensic data.

4.8 Knowledge of anti-forensics tactics, techniques and procedures (TTPS).

4.9 Knowledge of common forensic tool configuration and support applications (e.g., VMWare®, Wireshark®).

4.10 Knowledge of network traffic analysis methods.

4.11 Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.

DOMAIN 5: SECURITY IMPLICATIONS AND ADOPTION OF EVOLVING TECHNOLOGY

5.1 Knowledge of emerging technology and associated security issues, risks and vulnerabilities.

5.2 Knowledge of risk associated with mobile computing.

5.3 Knowledge of cloud concepts around data and collaboration.

5.4 Knowledge of risk of moving applications and infrastructure to the cloud.

5.5 Knowledge of risk associated with outsourcing.

5.6 Knowledge of supply chain risk management processes and practices.