Information Technology Security (ITS)
Competency Requirements

This competency listing serves to identify the major knowledge, skills, and standards areas which the Information Technology Security (**ITS**) specialist needs in order to perform the professional tasks associated with the development of security plans and processes for information technology and cybersecurity. An **ITS** should have prior computer systems and networking experience; prior certification in Information Technology and networking practices is highly suggested.

Information Technology Security specialists must be knowledgeable in the following technical areas:

1.0 Network Hardware Security Fundamentals

- 1.1 Define and explain network hardware firewalls:
  - 1.1.1 Identify how Network Address Translation (NAT) acts as a firewall
  - 1.1.2 Explain Packet Filtering and identify the differences between:
    - 1.1.2.1 Intrusion Detection Sensor (IDS)
    - 1.1.2.2 Intrusion Prevention Sensor (IPS)
  - 1.1.3 Stateful firewalls and characteristics
    - 1.1.3.1 Deep Packet Inspection (DPI)
    - 1.1.3.2 Medium Packet Inspection (MPI)
    - 1.1.3.3 Shallow Packet Inspection (SPI)
  - 1.1.4 Stateless Firewalls
- 1.2 Explain the use of gateway servers, routers, switches, Virtual Private Networks (VPNs) and proxy servers
  - 1.2.1 Differentiate between the following proxies:
    - 1.2.1.1 Reverse proxies
    - 1.2.1.2 Transparent proxies
    - 1.2.1.3 Anonymous proxies
    - 1.2.1.4 Highly anonymous proxies
    - 1.2.1.5 Socks 4 and 5 proxies
    - 1.2.1.6 Domain Name System (DNS) proxies
  - 1.2.2 Router and switch protection
    - 1.2.2.1 Explain how virtual local area networks (VLANs) can provide a very high level of security with flexibility
    - 1.2.2.2 Explain the IEEE 802.1Q standard specifying VLAN tagging to carry multiple VLANs on Ethernet links between switches
  - 1.2.3 Describe Internet Protocol packet Time To Live (IP TTL) security and how it is used by a network router
- 1.3 Explain a network “Demilitarized Zone” (DMZ) or perimeter network and why it is used
  - 1.3.1 Identify perimeter network services including:
    - 1.3.1.1 VPN
    - 1.3.1.2 Internet access
    - 1.3.1.3 Access to applications via LAN, WAN, Software Defined-WAN (SD-WAN) or cloud apps
- 1.4 Explain data redundancy and Redundant Array of Independent Disks (RAID)
  - 1.4.1 Identify how data redundancy can be implemented
    - 1.4.1.1 Explain server clustering
    - 1.4.1.2 Explain the use of failover cluster solutions
  - 1.4.2 List types of RAID arrays
- 1.5 Identify how to use embedded system security
  - 1.5.1 Describe security level access terminology

2.0 Physical Security

- 2.1 Explain how to set up physical security procedures for IT systems
  - 2.1.1 Explain what a physical “Demilitarized Zone” DMZ is and how deployed.
  - 2.1.2 Identify building site perimeter safeguards
    - 2.1.2.1 Fencing and security gates

- 2.1.2.2 Closed Circuit TV camera placement
- 2.1.2.3 Parking space surveillance
- 2.1.2.4 Explain how tailgating works
- 2.1.3 Identify Perimeter Intrusion Detection Systems (PIDS) and Prevention Systems (PS) including:
  - 2.1.3.1 Differentiate how PIDS and PS work
  - 2.1.3.2 Describe Distributed Acoustic Sensing (DAS)
- 2.1.4 Identify types of fire, power, temperature, weather and water/humidity protection

2.2 Explain how to develop and manage Redundant Power Supplies
- 2.2.1 Battery Backup
- 2.2.2 Uninterruptable Power Supplies (UPS)

2.3 Explain the “clean desk policy”

2.4 Identify physical security procedures and policies, including access control
- 2.4.1 Identify “Visitor” access procedures:
  - 2.4.1.1 biometric devices
  - 2.4.1.2 other security devices
- 2.4.2 Explain methods of network equipment physical security to include:
  - 2.4.2.1 enclosure security
  - 2.4.2.2 “Defense in Depth” strategy
  - 2.4.2.3 layered security
- 2.4.3 Describe use of data storage devices:
  - 2.4.3.1 thumb (jump, flash) drives
  - 2.4.3.2 secure digital (SD)/Micro SD cards
  - 2.4.3.3 optical data discs
- 2.4.4 Explain how passive radio-frequency identification (RFID) tags and near field communication (NFC) can be used for physical security
  - 2.4.4.1 Describe how RFID and NFC tags track items
  - 2.4.4.2 Explain how RFID technology can be incorporated into personnel ID cards

2.5 Identify how risks associated with “Dumpster Diving” can be mitigated

3.0 Network Software Security

3.1 Define and explain Software firewalls:
- 3.1.1 Application level firewalls
- 3.1.2 File scans
- 3.1.3 File Back-ups
- 3.1.4 Smart Firewalls
- 3.1.5 Download protection
- 3.1.6 Browser protection

3.2 Identify network protocols
- 3.2.1 Explain Transport Layer Security (TLS) protocol
- 3.2.2 Explain Internet Protocol Security (IPsec) components: Encapsulating Security Payload (ESP), Authentication Header (AH), Internet Key Exchange (IKE)
- 3.2.3 Explain Internet Control Message Protocol (ICMP)

3.3 Define the “OSI Model” and its relation to network security

3.4 Identify basic port numbers in regards to network security
- 3.4.1 Explain how to protect the ITU-T.120 protocol set, including Microsoft® Remote Desktop Protocol (RDP)

3.5 Describe how patch management relates to software security
- 3.5.1 Explain Service Pack
- 3.5.2 Explain “hotfix”

3.6 Identify antivirus, and anti-malware software suites
- 3.6.1 Describe how security software should be deployed

3.7 Identify methods to manage network access control
- 3.7.1 Describe the Lightweight Directory Access Protocol (LDAP) mapping feature and how to map users to certain roles within a network

- 3.7.2 Explain application whitelisting versus blacklisting for network system access
- 3.8 Describe "Domain Name System" (DNS) attack mitigations to include:
  - 3.8.1 Denial of Service (DoS)
  - 3.8.2 Distributed Denial of Service (DDoS)
  - 3.8.3 Cache Poisoning
  - 3.8.4 DNS Amplification
  - 3.8.5 Fast-flux DNS
  - 3.8.6 Zero Day Attack
- 3.9 Explain how TCP/IP Hijacking is accomplished and the accompanying attacks including:
  - 3.9.1 "Man-in-the-Middle" (MiTM)
    - 3.9.1.1 Address Resolution Protocol (ARP) Spoofing
    - 3.9.1.2 Replay attack
  - 3.9.2 TCP SYN (synchronize) Flood
  - 3.9.3 IP Spoofing
  - 3.9.4 TCP sequence number attack (prediction)
  - 3.9.5 TCP session hijacking
  - 3.9.6 RST/FIN Flood
- 3.10 Define (Remote Authentication Dial-In User Service) RADIUS protocol and how it is used by an enterprise or Internet service provider for Authentication, Access and Accounting
  - 3.10.1 Identify why RADIUS is used as the IEEE 802.1X back-end for authentication for LANs
- 3.11 Explain Structured Query language (SQL) access security procedures
  - 3.11.1 Identify the configuration of Internet Information Services (IIS) to access SQL Server
  - 3.11.2 Explain an SQL Injection attack
- 3.12 Explain how Simple Network Management Protocol (SNMP) is used on a network to share information with different devices securely
- 3.13 Identify security threats and best practices for maintaining secure operations and data assets in the cloud
  - 3.13.1 Software as a Service (SaaS)
  - 3.13.2 Platform as a Service (PaaS)
  - 3.13.3 Infrastructure as a Service (IaaS)

4.0 Wireless Security

- 4.1 Describe the IEEE wireless security standards
  - 4.1.1 Explain the purpose for wireless encryption keys
  - 4.1.2 "Temporal Key Integrity Protocol" (TKIP)
  - 4.1.3 "Advanced Encryption Standard" (AES)
  - 4.1.4 "Counter Mode with Cipher Block Chaining Message Authentication Code Protocol" (CCMP) (IEEE 802.11i)
  - 4.1.5 Explain how to change the Service Set Identifier (SSID)
- 4.2 Identify security best practices for wireless IoT networks
  - 4.2.1 Identify security precautions for mesh networks including Bluetooth®, ZigBee, RFID, Z-Wave®, and other 802.15.4 operations
  - 4.2.2 Explain Wi-Fi™ Protected Setup (WPS)
- 4.3 Identify and explain wireless network attack vectors
  - 4.3.1 "Evil Twin" counterfeit wireless access point (WAP)
  - 4.3.2 Identify site survey requirements to establish a wireless network
    - 4.3.2.1 Explain how to analyze and adjust wireless network frequencies
  - 4.3.3 Identify how to protect a network from mobile devices
    - 4.3.3.1 Identify how Single Sign On (SSO) technology works
- 4.4 Explain "Wireless Access Point" (WAP) technology and application
  - 4.4.1 Explain Wireless Transport Layer Security (WTLS)
  - 4.4.2 Describe these different types of IEEE wireless protocols:
    802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax
  - 4.4.3 Describe IEEE 802.1X and the "Extensible Authentication Protocol" (EAP)
  - 4.4.4 Describe wireless network security protocols:
    - 4.4.4.1 Wired Equivalent Privacy (WEP), (part of IEEE 802.11-1997)
    - 4.4.4.2 Wi-Fi™ Protected Access (WPA), (part of IEEE 802.11g-2003)
    - 4.4.4.3 Wi-Fi™ Protected Access II (WPA2), (IEEE 802.11i-2004)

5.0 Device Security

- 5.1 Identify security concepts that are needed with the development of Internet of Things (IoT)
  - 5.1.1 Identify attack vectors for sensors and other mesh connected devices for an IoT implementation and physical security.
  - 5.1.2 Identify methods used to protect the integrity of IoT devices.
    - 5.1.2.1 Device patching
    - 5.1.2.2 Media Access Control (MAC)
    - 5.1.2.3 Data Link Layer (DLL)
    - 5.1.2.4 Logical Link Control (LLC)
- 5.2 Describe the vulnerabilities associated with Bluetooth® technology
  - 5.2.1 Identify the Bluetooth® Device Address (BD_ADDR) is and how it can be exploited
  - 5.2.2 Identify the Bluetooth® Low Energy (BLE) applications
- 5.3 Explain the vulnerabilities of mobile devices and how to mitigate them
  - 5.3.1 Identify the dangers of iOS jail-braking
  - 5.3.2 Identify types of iOS and Android mobile malware
- 5.4 Identify possible attack vectors for device security

6.0 Software Exploitations and Vulnerabilities

- 6.1 Explain what malicious computer software code and/or applications are and how it can disrupt a computer's operation
  - 6.1.1 Identify how different malicious software code can affect computers including:
    - 6.1.1.1 Spyware
    - 6.1.1.2 Key loggers
    - 6.1.1.3 Viruses
      - 6.1.1.3.1 Boot sector
      - 6.1.1.3.2 Polymorphic
      - 6.1.1.3.3 Email
      - 6.1.1.3.4 Other macro
    - 6.1.1.4 Logic bombs
    - 6.1.1.5 Worms
    - 6.1.1.6 Trojans
    - 6.1.1.7 Malware, such as Adware
    - 6.1.1.8 Other malicious code that infiltrates a computer
  - 6.1.2 Explain how a "botnet" works across a network
  - 6.1.3 Explain Ransomware and how it used
  - 6.1.4 Identify how a Back Door is used
  - 6.1.5 Explain the concept of "Reverse Shells" within a network
  - 6.1.6 Explain "Weak Keys" and "Password Guessing"
  - 6.1.7 Identify steganography techniques used to thwart security measures
- 6.2 Explain and describe different attack vectors on a network
  - 6.2.1 Explain how advanced persistent threats are orchestrated and how they can affect a network
- 6.3 Identify how the Common Vulnerabilities and Exposures (CVE) system works to reference information-security vulnerabilities

7.0 Operational Standards, Policies and Risk Assessments

- 7.1 Identify national and international cyber security standards
  - 7.1.1 ISO/IEC 27001:2013 (Information Security Management Standards)
  - 7.1.2 ISO/IEC 27103-2018 (I.T.-Security techniques-Cybersecurity Standards)
  - 7.1.3 ISO/IEC 27032-2012 (Guidelines for Cyber Security)
  - 7.1.4 IEEE 1686-2013 (Intelligent Electronic Devices Cyber Security Capabilities)
  - 7.1.5 Be aware of :
    - 7.1.5.1 National Institute for Standards and Technology (NIST) 800-53, recommended security controls
    - 7.1.5.2 Center for Internet Security (CIS) Benchmarks
    - 7.1.5.3 Sarbanes-Oxley (SOX) Compliance requirements
    - 7.1.5.4 Payment Card Industry – Data Security standards (PCI-DSS)
    - 7.1.5.5 HIPPA compliance requirements

- 7.2 Identify forms of risk in security management
  - 7.2.1 Explain how a risk assessment plan works
  - 7.2.2 Identify risk mitigation procedures
    - 7.2.2.1 Explain risk monitoring and control
  - 7.2.3 Be aware of:
    - 7.2.3.1 Risk Management Framework (RMF)
    - 7.2.3.2 Federal Risk and Authorization Management Program (FedRAMP)
- 7.3 Explain different forms of operational standards and policies to mitigate risk
  - 7.3.1 Identify access authentication policies and procedures
  - 7.3.2 Identify access authorization policies
- 7.4 Identify network exposure factors and how to calculate potential loss
- 7.5 Explain operational security controls and how they work
- 7.6 Explain methods that can be used to detect attackers activities on a network
  - 7.6.1 Identify how honey nets and honeypots can be used to detect and identify network intruders
- 7.7 Describe network security tools and procedures to:
  - 7.7.1 Identify tools used to safeguards against attacks
  - 7.7.2 Identify software used to monitor activities
- 7.8 Identify backup tools used in safeguarding critical resources to include:
  - 7.8.1 software
  - 7.8.2 hardware
- 7.9 Explain Transport Layer and Secure Socket Layer (SSL) in network cybersecurity including the Hyper Text Transport Protocol over Secure Socket layer (HTTPS)
  - 7.9.1 Identify other network communications security protocols

8.0 Disaster Recovery and Computer Forensics

- 8.1 Identify and describe the different forms of data classification
- 8.2 Identify key points required for a typical network enterprise disaster plan
- 8.3 Explain the components of a disaster recovery plan and the order they are developed
  - 8.3.1 Continuity of Operations Planning (COOP)
    - 8.3.1.1 Back-up sites: “Hot site”, “Warm site”, “Cold Site”
  - 8.3.2 Secure recovery
- 8.4 Identify back-up and recovery procedures
- 8.5 Explain succession planning
- 8.6 Explain computer forensics (cyberforensics) and how it is used
  - 8.6.1 Cross-drive analysis (CDA)
  - 8.6.2 Forensic feature extraction (FFE)
  - 8.6.3 Live analysis
- 8.7 Explain attack incident handling procedures
  - 8.7.1 Identify the responsibilities of a “Computer Incident Response Team” (CIRT)

9.0 Cryptography

- 9.1 Identify the three types of authentication:
  - 9.1.1 Password
  - 9.1.2 Blocker tag (RSA®)/smartcard
  - 9.1.3 Biometrics
- 9.2 Explain asymmetric and symmetric style key encryption including:
  - 9.2.1 Cryptography and encryption algorithms
    - 9.2.1.1 Explain encryption technologies and block ciphers such as Two Fish, Blowfish, AES, DES (Data Encryption Standard), 3DES
    - 9.2.1.2 Identify stream ciphers, SALSA, SOSEMANUK, PANAMA
  - 9.2.2 Hashing
    - 9.2.2.1 Describe Secure Hash Algorithm (SHA) and SHA-1
    - 9.2.2.2 Define MD5 (Message Digest 5) collisions
- 9.3 Explain Public Key Infrastructure (PKI) of the X.509 standard including:
  - 9.3.1 trust models and certificate authority
  - 9.3.2 (digital) certificates and revocation
  - 9.3.3 M of N (Minimum of [total] Number) control environment
- 9.4 Explain PGP (Pretty Good Privacy)(Source of Certificate Authorities)

9.5 Explain in depth knowledge of multi-factor authentication
9.6 Explain why Time To Live (TTL) security is used to protect against forged IP packet attacks

10.0 Social Engineering

10.1 Explain the different types of social engineering attacks
  10.1.1 Identify processes involved in:
    10.1.1.1 Phishing attacks, (Smishing, Vishing)
    10.1.1.2 Baiting
    10.1.1.3 Pretexting
    10.1.1.4 Scareware attacks
    10.1.1.5 Email spoofing
    10.1.1.6 Advanced Persistent Threats
    10.1.1.7 Watering hole attack
    10.1.1.8 Intimidation
  10.1.2 Explain “quid pro quo”
10.2 Identify methods and tools for countering social engineering attacks
  10.2.1 Identify how employee training and awareness programs can counter social engineering practices
10.3 Explain internet social engineering principles used in psychological manipulation

End of Information Technology Security Competency

Find An ETA Test Site: **http://www.eta-i.org/testing.html**

Suggested Additional Resource and Study Material:

As with most networking systems, you will find details and information on Websites: https://www.us-cert.gov/ncas/tips/ST17-001; https://www.consumer.ftc.gov/topics/identity-theft; dhs.gov; nist.gov; ieee.org; sans.org, (sans.edu); sae.org; rsa.com (blogs.rsa.com); schneier.com, security.intuit.com; networkcomputing.com; cisco.com; pcworld.com; cnet.com; computerworld.com; pcmag.com; consumerreports.org; maximumpc.com; infoworld.com; microsoft.com; itunes.apple.com; rmroberts.com; professormesser.com; youtube.com; and many, many other websites.

Cybersecurity Essentials, 1st Ed; Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short; ISBN 978-1119362395; Sybex; Oct.2018; 784 pgs

ITS By The Numbers; T. Houser, Michael Goshen; Self Publishing; 2017; ebook & softcover;

Cyber Reconnaissance, Surveillance and Defense; Robert Shimonski; ISBN 978-0128013083; Syngress; 2014; softcover; 258 pgs

Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information; Michael Bazzell; ISBN 978- 1530508907; Create Space Publishing; 2016; softcover; 422 pgs.

Cybersecurity and Cyberwar: What Everyone Needs to Know; P.W. Singer, Allan Friedman; ISBN 978-0199918119; Oxford Univ. Press; 2014; softcover; 320 pgs.

Thinking Security: Stopping Next Year's Hackers; Steven Bellovin; ISBN 978-0134277547; Addison-Wesley Professional Computing Series; Nov.2015; hardcover; 400 pgs.

Information Technology Security Specialist Committee Advisory Board:

Brooks, Chuck	chuck@eitprep.com
Capano, Daniel, CWSP	dcapano@sbcglobal.net
Carnahan, Shane	ryan.s.carnahan22@gmail.com
Carr, Frederick,	fwcarr@gmail.com
Copeland, Joshua CST, NST	jdcopeland@gmail.com
Coulombe, Ray ITS, ESNT	ray@securityspecifiers.com
Gonzales, Brandon CETsr	bsgonzales@bsu.edu
Goshen, Michael, CST, ITS, NST	goshen@michaelgoshen.com
Groves, J.B., III, ITS, FOT, (many more)	jbgroves@wcjc.edu
Ingram. Eric, CETsr, FOT	eingram2@brandman.edu
Kirkpatrick, Ed, PV2, PVI, CSS	ekirkpatrick@eta-i.org
Kirschbaum, Tim, NST, CST, FOT	kirschbaumt@hotmail.com
Klier, Brian	brian.klier@gmail.com
Moran, Bruce	bruce@totalrecallpress.com

ETA certification programs are accredited through ICAC, complying with the ISO/IEC 17024 standard.

