

NSA/DHS CAE in IA/CD
2014 Mandatory Knowledge Unit Checklist – 4 Year⁺ Programs

Mandatory Knowledge Units

1.0 Core2Y

1.1 Basic Data Analysis

The intent of this Knowledge Unit is to provide students with basic abilities to manipulate data into meaningful information.

1.1.1 Topics

- ___ Summary Statistics
- ___ Graphing / Charts
- ___ Spreadsheet Functions
- ___ Problem solving

1.1.2 Outcomes

- Students will be able to:
- ___ Apply standard statistical inference procedures to draw conclusions from data.

1.2 Basic Scripting or Introductory Programming

The intent of this Knowledge Unit is to provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

1.2.1 Topics

- ___ *Basic Security
 - ___ Bounds checking, input validation
- ___ Program Commands
- ___ Program Control Structures
- ___ Variable Declaration
- ___ Debugging
- ___ Scripting Language (e.g. PERL, Python, BASH, VB Scripting, Powershell)
- ___ *Basic Boolean logic/operations
 - ___ AND / OR / XOR / NOT

1.2.2 Outcomes

- Students will be able to:
- ___ Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks).
 - ___ Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
 - ___ Write simple linear and looping scripts.

1.3 Cyber Defense

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

1.3.1 Topics:

- ___ Network mapping (enumeration and identification of network components)
- ___ *Network security techniques and components
 - ___ Access controls, flow control, cryptography, firewalls, intrusion detection systems, etc.
- ___ Applications of Cryptography

* = Can include a summary justification for that section.

2014 Mandatory Knowledge Unit Checklist – 4 Year⁺ Programs

- ___ Malicious activity detection / forms of attack
- ___ Appropriate Countermeasures
- ___ Trust relationships
- ___ *Defense in Depth
 - ___ Layering of security mechanisms to achieve desired security
- ___ *Patching
 - ___ OS and Application Updates
- ___ Vulnerability Scanning
- ___ Vulnerability Windows (0-day to patch availability)

1.3.2 Outcomes:

Students will be able to:

- ___ Describe potential system attacks and the actors that might perform them
- ___ Describe cyber defense tools, methods and components
- ___ Apply cyber defense methods to prepare a system to repel attacks
- ___ Describe appropriate measures to be taken should a system compromise occur.

1.4 Cyber Threats

The intent of this Knowledge Unit is to provide students with basic information about the threats that may be present in the cyber realm.

1.4.1 Topics:

- ___ Adversaries and targets
- ___ Motivations and Techniques
- ___ The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access)
- ___ *Types of Attacks
 - ___ Password guessing / cracking
 - ___ Backdoors / trojans / viruses / wireless attacks
 - ___ Sniffing / spoofing / session hijacking
 - ___ Denial of service / distributed DOS / BOTs
 - ___ MAC spoofing / web app attacks / 0-day exploits
 - ___ Vulnerabilities that enable attacks
- ___ Attack Timing (within x minutes of being attached to the net)
- ___ Social Engineering
- ___ Events that indicate an attack is/has happened
- ___ Legal Issues
- ___ Attack surfaces / vectors
- ___ Attack trees
- ___ Insider problem
- ___ Covert Channels
- ___ Threat Information Sources (e.g., CERT)

1.4.2 Outcomes:

Students will be able to:

- ___ Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk
- ___ Describe different types of attacks and their characteristics

* = Can include a summary justification for that section.

2014 Mandatory Knowledge Unit Checklist – 4 Year⁺ Programs

1.5 Fundamental Security Design Principles

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

1.5.1 Topics:

- Separation (of domains)
- Isolation
- Encapsulation
- Least Privilege
- Simplicity (of design)
- Minimization (of implementation)
- Fail Safe Defaults / Fail Secure
- Modularity
- Layering
- Least Astonishment
- Open Design
- Usability

1.5.1 Outcomes:

Students will be able to:

- List the first principles of security
- Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies
- Analyze common security failures and identify specific design principles that have been violated
- Identify the needed design principle when given a specific scenario
- Describe why good human machine interfaces are important to system use
- Understand the interaction between security and system usability and the importance for minimizing the affects of security mechanisms

1.6 Information Assurance Fundamentals

The intent of this Knowledge Unit is to provide students with basic concepts of information assurance fundamentals.

1.6.1 Topics

- Threats and Adversaries
- Vulnerabilities and Risks
- Basic Risk Assessment
- Security Life-Cycle
- Intrusion Detection and Prevention Systems
- Cryptography
- Data Security (in transmission, at rest, in processing)
- Security Models
- Access Control Models (MAC, DAC, RBAC)
- Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
- Security Mechanisms (e.g., Identification/Authentication, Audit)

* = Can include a summary justification for that section.

2014 Mandatory Knowledge Unit Checklist – 4 Year⁺ Programs

1.6.2 Outcomes

Students will be able to:

- ___ List the fundamental concepts of the Information Assurance / Cyber Defense discipline
- ___ Describe how the fundamental concepts of cyber defense can be used to provide system security
- ___ Examine the architecture of a typical, complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed

1.7 Introduction to Cryptography

The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.

1.7.1 Topics

- ___ Symmetric Cryptography (DES, Twofish)
- ___ *Public Key Cryptography
 - ___ Public Key Infrastructure
 - ___ Certificates
- ___ *Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3)
 - ___ For integrity
 - ___ For protecting authentication data
 - ___ Collision resistance
- ___ Digital Signatures (Authentication)
- ___ Key Management (creation, exchange/distribution)
- ___ Cryptographic Modes (and their strengths and weaknesses)
- ___ Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.)
- ___ Common Cryptographic Protocols
- ___ DES -> AES (evolution from DES to AES)
- ___ Security Functions (data protection, data integrity, authentication)

1.7.2 Outcomes

Students will be able to:

- ___ Identify the elements of a cryptographic system
- ___ Describe the differences between symmetric and asymmetric algorithms
- ___ Describe which cryptographic protocols, tools and techniques are appropriate for a given situation
- ___ Describe how crypto can be used, strengths and weaknesses, modes, and the issues that must be addressed in an implementation (e.g., key management), etc

1.8 Information Technology System Components

The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

1.8.1 Topics

- ___ Workstations
- ___ Servers
- ___ Network Storage Devices
- ___ Routers / Switches / Gateways

* = Can include a summary justification for that section.

2014 Mandatory Knowledge Unit Checklist – 4 Year⁺ Programs

- Guards / CDSes / VPNs / Firewalls
- IDSes, IPSes
- Mobile Devices
- Peripheral Devices / Security Peripherals

1.8.2 Outcomes

Students will be able to:

- Describe the hardware components of modern computing environments and their individual functions

1.9 Networking Concepts

The intent of this Knowledge Unit is to provide students with basic understanding of network components and how they interact.

1.9.1 Topics

- Overview of Networking (OSI Model)
- Network Media
- Network architectures (LANs, WANs)
- Network Devices (Routers, Switches, VPNs, Firewalls)
- Network Services
- Network Protocols (TCP/IP, HTTP, DNS, SMTP, UDP)
- Network Topologies
- Overview of Network Security Issues

1.9.2 Outcomes

Students will be able to:

- Describe the fundamental concepts, technologies, components and issues related to communications and data networks.
- Describe a basic network architecture given a specific need and set of hosts/clients.
- Track and identify the packets involved in a simple TCP connection (or a trace of such a connection).
- Use a network monitoring tool (e.g., WireShark).
- Use a network mapping tool (e.g., Nmap).

1.10 Policy, Legal, Ethics and Compliance

The intent of this Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.

1.10.1 Topics

- HIPAA / FERPA
- Computer Security Act
- Sarbanes – Oxley
- Gramm – Leach – Bliley
- Privacy (COPPA)
- Payment Card Industry Data Security Standard (PCI DSS)
- State, US and international standards / jurisdictions
- Laws and Authorities
- US Patriot Act
- BYOD issues

* = Can include a summary justification for that section.

2014 Mandatory Knowledge Unit Checklist – 4 Year⁺ Programs

____ Americans with Disabilities Act, Section 508

1.10.2 Outcomes

Students will be able to:

- ____ List the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data
- ____ Describe their responsibilities related to the handling of information about vulnerabilities
- ____ Describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it

1.11 Systems Administration

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

1.11.1 Topics

- ____ OS Installation
- ____ User accounts management
- ____ Password policies
- ____ Authentications Methods
- ____ Command Line Interfaces
- ____ Configuration Management
- ____ Updates and patches
- ____ Access Controls
- ____ Logging and Auditing (for performance and security)
- ____ Managing System Services
- ____ Virtualization
- ____ Backup and Restoring Data
- ____ File System Security
- ____ Network Configuration (port security)
- ____ Host (Workstation/Server) Intrusion Detection
- ____ Security Policy Development

1.11.2 Outcomes

Students will be able to:

- ____ Apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup

2.0 Core to 4 year⁺ only

2.1 Database Management Systems

The intent of this Knowledge Unit is to provide students with the skills to utilize database management system to solve specific problems.

2.1.1 Topics

- ____ Overview of database types (e.g., flat, relational, network, object-oriented)
- ____ SQL (for queries)
- ____ Advanced SQL (for DBMS administration – e.g., user creation/deletion, permissions and access controls)

* = Can include a summary justification for that section.

2014 Mandatory Knowledge Unit Checklist – 4 Year⁺ Programs

- ___ Indexing, Inference, Aggregation, Polyinstantiation
- ___ How to protect data (confidentiality, integrity and availability in a DBMS context)
- ___ Vulnerabilities (e.g., SQL injection)

2.1.2 Outcomes

Students will be able to:

- ___ List the most common structures for storing data in a database management system
- ___ Configure a commodity DBMS for secure access
- ___ Describe alternatives to relational DBMSs and their unique security issues
- ___ Describe the role of a database, a DBMS, and a database server within a complex system supporting multiple applications
- ___ Demonstrate basic SQL proficiency for table creation, data insertion and data query
- ___ Describe DBMS access controls and privilege levels and apply them to a simple database
- ___ Develop a DB structure for a specific system/problem.

2.2 Network Defense

The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.

2.2.1 Topics

- ___ Implementing IDS/IPS
- ___ Implementing Firewalls and VPNs
- ___ Defense in Depth
- ___ Honeypots and Honeynets
- ___ Network Monitoring
- ___ Network Traffic Analysis
- ___ Minimizing Exposure (Attack Surface and Vectors)
- ___ Network Access Control (internal and external)
- ___ DMZs / Proxy Servers
- ___ Network Hardening
- ___ Mission Assurance
- ___ Network Policy Development and Enforcement
- ___ Network Operational Procedures
- ___ Network Attacks (e.g., session hijacking, Man-in-the-Middle)

2.1.2 Outcomes

Students will be able to:

- ___ Describe the various concepts in network defense.
- ___ Apply their knowledge to implement network defense measures.
- ___ Use a network monitoring tools (e.g., WireShark).
- ___ Use a network mapping tool (e.g., Nmap).

2.3 Network Technology and Protocols

The intent of this Knowledge Unit is to provide students with an understanding of the components in a network environment, their roles, and communication methods.

2.3.1 Topics

- ___ Network Architectures
- ___ Networks Infrastructure

* = Can include a summary justification for that section.

2014 Mandatory Knowledge Unit Checklist – 4 Year⁺ Programs

- Network Services
- Network Protocols (TCP/IP – v4 and v6, DNS, HTTP, SSL, TLS)
- Network Address Translation and Sub-netting
- Network Analysis/Troubleshooting
- Network Evolution (Change Management, BYOD)
- Remote and Distributed Management

2.3.2 Outcomes

Students will be able to:

- Apply their knowledge of network technologies to design and construct a working network
- Analyze a trace of packets to identify the establishment of a TCP connection
- Demonstrate the use of a network monitor to display packets

2.4 Operating Systems Concepts

The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

2.4.1 Topics

- Privileged and non-privileged states
- Processes and Threads (and their management)
- Memory (real, virtual, and management)
- Files Systems
- *Access Controls (Models and Mechanisms)
 - Access control lists
- Virtualization / Hypervisors
- How does the an OS protect itself from attack?
- *Fundamental Security Design Principles as applied to an OS
 - Domain separation, process isolation, resource encapsulation, least privilege

2.4.2 Outcomes

Students will be able to:

- Identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)

2.5 Probability and Statistics

The intent of this Knowledge Unit is to provide students with the ability to use basic statistics to analyze and attach meaning to datasets.

2.5.1 Topics

- Probability as a concept
- Random variables/events
- Odds of an event happening
- Data Interpretation
- Statistical Problem Solving
- Probability Distributions

2.5.2 Outcomes

Students will be able to:

- Evaluate probabilities to solve applied problems
- Describe how basic statistics and statistical methods can be applied in a given situation

* = Can include a summary justification for that section.

2014 Mandatory Knowledge Unit Checklist – 4 Year⁺ Programs

2.6 Programming

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

2.6.1 Topics

- ___ Programming Language, such as: C
- ___ Programming constructs and concepts variables, strings, assignments, sequential execution, loops, functions
- ___ Security issues, such as type checking and parameter validation
- ___ *Basic Boolean logic/operations
 - ___ AND / OR / XOR / NOT

2.6.2 Outcomes

Students will be able to:

- ___ Demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner
- ___ Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL)
- ___ Demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web)

* = Can include a summary justification for that section.