

Centers of Academic Excellence in Cyber Defense (CAE-CD) Specializations

Cyber Investigations.....	2
Data Management Systems Security.....	3
Data Security Analysis.....	4
Digital Forensics	5
Health Care Security	6
Industrial Control Systems-SCADA Security	7
Network Security Administration	8
Network Security Engineering	9
Secure Cloud Computing	10
Secure Embedded Systems.....	11
Secure Mobile Technology	12
Secure Software Development.....	13
Secure Telecommunications	14
Security Incident Analysis and Response	15
Security Policy Development and Compliance.....	16
System Security Administration.....	17
Systems Security Engineering.....	18

Cyber Investigations

KUs necessary to impart the necessary skills and abilities for performing technical analyses of computer incidents and intrusions to determine source, infiltration path, mechanism, system modifications and effects, damages, exfiltration path, data infiltrated, and residual effects.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Networking
- **Non-Technical Core KUs**
 - Cyber Threats
 - Policy, Legal, Ethics, and Compliance
 - Security Risk Analysis
- **Optional KUs**
 - Cyber Crime
 - Cybersecurity Ethics
 - Forensic Accounting
 - Fraud Prevention and Management
 - IA Compliance
 - Privacy

Data Management Systems Security

KUs necessary to impart the necessary skills and abilities for the secure configuration, operation and maintenance of databases and database management systems housing sensitive data.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Basic Networking
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
 - Cybersecurity Planning and Management
 - Policy, Legal, Ethics, and Compliance
 - Security Risk Analysis
- **Optional KUs**
 - Cloud Computing
 - Data Administration
 - Database Management Systems
 - Databases
 - IA Compliance
 - Secure Programming Practices
 - Linux System Administration
 - Windows System Administration

Data Security Analysis

KUs necessary to impart the necessary skills and abilities for the analysis of data (e.g., system logs, network traffic) to identify suspected malicious activities.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Scripting and Programming
 - Basic Networking
- **Non-Technical Core KUs**
 - Security Program Management
 - Security Risk Analysis
- **Optional KUs**
 - Data Administration
 - Databases
 - IA Architectures
 - IA Compliance
 - Intrusion Detection/Prevention Systems
 - Systems Security Engineering
 - Wireless Sensor Networks

Digital Forensics

KUs necessary to impart the necessary skills and abilities for the analysis of computer systems (hosts, servers, network components) to determine the effects that malware has had on the system.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Basic Networking
 - Basic Scripting and Programming
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Policy, Legal, Ethics, and Compliance
- **Optional KUs**
 - Data Structures
 - Digital Forensics
 - Device Forensics
 - Host Forensics
 - Media Forensics
 - Network Forensics
 - Forensic Accounting
 - Hardware Reverse Engineering
 - Linux System Administration
 - Network Technology and Protocols
 - Operating Systems Theory
 - Software Reverse Engineering
 - Vulnerability Analysis
 - Windows System Administration

Health Care Security

KUs necessary to impart the necessary skills and abilities for the design, development, operation and maintenance of computer systems used in health care applications.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Basic Networking
 - Network Defense
- **Non-Technical Core KUs**
 - Cyber Threats
 - Policy, Legal, Ethics, and Compliance
 - Security Program Management
- **Optional KUs**
 - Data Administration
 - Database Management Systems
 - Databases
 - IA Compliance
 - IA Standards
 - Life-Cycle Security
 - Linux System Administration
 - Software Security Analysis
 - Supply Chain Security
 - Windows System Administration

Industrial Control Systems-SCADA Security

KUs necessary to impart the necessary skills and abilities for the design, development, operation and maintenance of industrial control systems used in critical infrastructures (e.g., finance, transportation, energy)

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Networking
 - Network Defense
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
 - Cybersecurity Planning and Management
 - Security Risk Analysis
- **Optional KUs**
 - Embedded Systems
 - Hardware/Firmware Security
 - Industrial Control Systems
 - Intrusion Detection/Prevention Systems
 - Linux System Administration
 - Network Technology and Protocols
 - Operating Systems Hardening
 - Secure Programming Practices
 - Systems Security Engineering
 - Vulnerability Analysis
 - Windows System Administration

Network Security Administration

KUs necessary to impart the necessary skills and abilities for the secure configuration, operation and operation of an enterprise computer network (to include infrastructure devices, network services and the servers upon which they run).

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Network Defense
 - Basic Networking
- **Non-Technical Core KUs**
 - Cyber Threats
 - Policy, Legal, Ethics, and Compliance
- **Optional KUs**
 - Advanced Network Technology and Protocols
 - Digital Forensics
 - Intrusion Detection/Prevention Systems
 - Life-Cycle Security
 - Network Forensics
 - Network Security Administration
 - Network Technology and Protocols
 - Penetration Testing
 - Supply Chain Security
 - Systems Certification and Accreditation
 - Vulnerability Analysis

Network Security Engineering

KUs necessary to impart the necessary skills and abilities for the design of secure network infrastructures and security analysis of network traffic

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Network Defense
 - Basic Networking
 - Basic Scripting and Programming
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
- **Optional KUs**
 - Advanced Cryptography
 - Advanced Network Technology and Protocols
 - Analog Telecommunications
 - Digital Communications
 - Digital Forensics
 - Life-Cycle Security
 - Mobile Technologies
 - Network Forensics
 - Network Security Administration
 - Network Technology and Protocols
 - Penetration Testing
 - Radio Frequency Principles
 - Systems Security Engineering
 - Vulnerability Analysis

Secure Cloud Computing

KUs necessary to impart the necessary skills and abilities for the design, development, operation and maintenance of secure cloud architectures.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Basic Networking
 - Basic Scripting and Programming
 - Network Defense
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
 - Policy, Legal, Ethics, and Compliance
 - Security Risk Analysis
- **Optional KUs**
 - Advanced Cryptography
 - Advanced Network Technology and Protocols
 - Cloud Computing
 - IA Compliance
 - Life-Cycle Security
 - Linux System Administration
 - Network Security Administration
 - Network Technology and Protocols
 - Operating Systems Hardening
 - Operating Systems Theory
 - Supply Chain Security
 - Virtualization Technologies
 - Vulnerability Analysis
 - Windows System Administration

Secure Embedded Systems

KUs necessary to impart the necessary skills and abilities for the design, development, analysis and secure use of embedded systems technologies.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Network Defense
 - Basic Networking
 - Basic Scripting and Programming
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
 - Policy, Legal, Ethics, and Compliance
- **Optional KUs**
 - Embedded Systems
 - Hardware/Firmware Security
 - Life-Cycle Security
 - Low Level Programming
 - Network Technology and Protocols
 - QA/Functional Testing
 - Secure Programming Practices

Secure Mobile Technology

KUs necessary to impart the necessary skills and abilities for the secure design, development, utilization and management of mobile technologies, devices and services.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Networking
- **Non-Technical Core KUs**
 - Cyber Threats
 - Policy, Legal, Ethics, and Compliance
 - Security Risk Analysis
- **Optional KUs**
 - Advanced Network Technology and Protocols
 - Data Structures
 - Digital Communications
 - Digital Forensics
 - Device Forensics
 - Network Forensics
 - Hardware/Firmware Security
 - IA Compliance
 - IA Standards
 - Life-Cycle Security
 - Mobile Technologies
 - Network Technology and Protocols
 - Radio Frequency Principles
 - Secure Programming Practices
 - Supply Chain Security
 - Systems Programming
 - Wireless Sensor Networks

Secure Software Development

KUs necessary to impart the necessary skills and abilities for the development of secure software (i.e., software that performs only its intended functions without the presence of exploitable vulnerabilities).

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Network Defense
 - Basic Networking
 - Basic Scripting and Programming
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
- **Optional KUs**
 - Algorithms
 - Data Structures
 - Formal Methods
 - Secure Programming Practices
 - Software Assurance
 - Software Security Analysis
 - Vulnerability Analysis

Secure Telecommunications

KUs necessary to impart the necessary skills and abilities for the design, development and secure use of secure telecommunications systems, digital and analog.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Network Defense
 - Basic Networking
 - Basic Scripting and Programming
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
 - Policy, Legal, Ethics, and Compliance
- **Optional KUs**
 - Advanced Network Technology and Protocols
 - Analog Telecommunications
 - Digital Communications
 - Digital Forensics
 - Network Forensics
 - Life-Cycle Security
 - Low Level Programming
 - Mobile Technologies
 - Network Security Administration
 - Network Technology and Protocols
 - Radio Frequency Principles
 - Supply Chain Security
 - Systems Programming
 - Systems Security Engineering

Security Incident Analysis and Response

KUs necessary to impart the necessary skills and abilities for analyzing security incidents on a system or network to determine the weakness (technological or operational) that allowed the incident to occur and developing appropriate mitigations to prevent further incidents via that weakness.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Network Defense
 - Basic Networking
 - Basic Scripting and Programming
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
 - Cybersecurity Planning and Management
- **Optional KUs**
 - Digital Forensics
 - Device Forensics
 - Host Forensics
 - Media Forensics
 - Network Forensics
 - IA Architectures
 - IA Compliance
 - IA Standards
 - Life-Cycle Security
 - Linux System Administration
 - Network Technology and Protocols
 - Operating Systems Hardening
 - Overview of Cyber Operations
 - Supply Chain Security
 - Vulnerability Analysis
 - Windows System Administration

Security Policy Development and Compliance

KUs necessary to impart the necessary skills and abilities for the development of organizational policies related to information assurance / cyber defense and the analysis of operational systems for compliance with applicable IA/CD-related laws and policies.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - None
- **Non-Technical Core KUs**
 - Cyber Threats
 - Cybersecurity Planning and Management
 - Policy, Legal, Ethics, and Compliance
 - Security Program Management
 - Security Risk Analysis
- **Optional KUs**
 - IA Architectures
 - IA Compliance
 - IA Standards
 - Life-Cycle Security
 - Linux System Administration
 - Supply Chain Security
 - Windows System Administration

System Security Administration

KUs necessary to impart the necessary skills and abilities for the secure configuration, operation and maintenance of a computer system (host or workstation).

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Network Defense
 - Basic Networking
 - Basic Scripting and Programming
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
 - Security Risk Analysis
- **Optional KUs**
 - Digital Forensics
 - Host Forensics
 - IA Architectures
 - IA Compliance
 - IA Standards
 - Intrusion Detection/Prevention Systems
 - Life-Cycle Security
 - Linux System Administration
 - Network Security Administration
 - Network Technology and Protocols
 - Operating Systems Hardening
 - Supply Chain Security
 - Systems Certification and Accreditation
 - Systems Security Engineering
 - Vulnerability Analysis
 - Windows System Administration

Systems Security Engineering

KUs necessary to impart the necessary skills and abilities for the development of secure systems from original idea through its entire lifecycle; this includes requirements definition, allocation of security mechanisms to system components for most effective and efficient implementation to satisfy the requirements, to development, operation, maintenance, and disposition of the system.

To complete this specialization area, you must complete the Technical Core, Non-Technical Core, and Optional KUs indicated below.

Knowledge Units

- **Technical Core KUs**
 - Basic Cryptography
 - Network Defense
 - Basic Networking
 - Basic Scripting and Programming
 - Operating Systems Concepts
- **Non-Technical Core KUs**
 - Cyber Threats
 - Security Risk Analysis
- **Optional KUs**
 - Advanced Network Technology and Protocols
 - Data Structures
 - IA Architectures
 - IA Standards
 - Life-Cycle Security
 - Low Level Programming
 - Network Technology and Protocols
 - Operating Systems Hardening
 - QA/Functional Testing
 - Supply Chain Security
 - Systems Programming
 - Systems Security Engineering
 - Virtualization Technologies