# NSA/DHS Centers of Academic Excellence for Information Assurance/Cyber Defense

## Focus Areas

Cyber Investigations

Data Management Systems Security

Data Security Analysis

Digital Forensics

Health Care Security

Industrial Control Systems – SCADA Security

Network Security Administration

Network Security Engineering

Secure Cloud Computing

Secure Embedded Systems

Secure Mobile Technology

Secure Software Development

Secure Telecommunications

Security Incident Analysis and Response

Security Policy Development and Compliance

Systems Security Administration

Systems Security Engineering

Focus Areas are for use with the CAE IA/CD Knowledge Units document.

## Cyber Investigations

This Focus Area encompasses the Knowledge Units 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 exfiltrated, and residual effects.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Data Analysis
- Cyber Threats
- IA Fundamentals
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- None

**This Focus Area requires the following optional Knowledge Units:**

- Digital Investigations
- Forensic Accounting
- Fraud Prevention and Management
- IA Compliance
- Security Risk Analysis

## Data Management Systems Security

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the secure configuration, operation and maintenance of databases and database management systems housing sensitive data.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Database Management Systems
- Operating Systems Concepts

**This Focus Area requires the following optional Knowledge Units:**

- Cloud Computing
- Cybersecurity Planning and Management
- Data Administration
- Databases
- IA Compliance
- Secure Programming Practices
- Security Risk Analysis

## Data Security Analysis

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the analysis of data (e.g., system logs, network traffic) to identify suspected malicious activities.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Data Analysis
- Basic Scripting or Introductory Programming
- Fundamental Security Design Principles
- Networking Concepts

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Database Management Systems
- Probability and Statistics

**This Focus Area requires the following optional Knowledge Units:**

- Data Administration
- IA Architectures
- IA Compliance
- Intrusion Detection
- Security Program Management
- Security Risk Analysis
- Systems Engineering
- Wireless Sensor Networks

## Digital Forensics

This Focus Area encompasses the Knowledge Units 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.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Scripting or Introductory Programming
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Networking Technology and Protocols
- Operating Systems Concepts

**This Focus Area requires the following optional Knowledge Units:**

- Data Structures
- Device Forensics
- Digital Investigations
- Forensic Accounting
- Hardware Reverse Engineering
- Host Forensics
- Media Forensics
- Network Forensics
- Operating Systems Theory
- Software Reverse Engineering
- Vulnerability Analysis

## Health Care Security

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the design, development, operation and maintenance of computer systems used in health care applications.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Database Management Systems
- Network Defense

**This Focus Area requires the following optional Knowledge Units:**

- Data Administration
- Databases
- IA Compliance
- IA Standards
- Life-Cycle Security
- Security Program Management
- Software Security Analysis
- Supply Chain Security

## Industrial Control Systems/SCADA Security

This Focus Area encompasses the Knowledge Units 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).

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- IT Systems Components
- Networking Concepts
- System Administration

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Network Defense
- Networking Technology and Protocols
- Operating Systems Concepts

**This Focus Area requires the following optional Knowledge Units:**

- Cybersecurity Planning and Management
- Embedded Systems
- Hardware/Firmware Security
- Industrial Control Systems
- Intrusion Detection
- Operating Systems Hardening
- Secure Programming Practices
- Security Risk Analysis
- Systems Engineering
- Vulnerability Analysis

## Network Security Administration

This Focus Area encompasses the Knowledge Units 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).

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Scripting or Introductory Programming
- Cyber Threats
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Network Defense
- Networking Technology and Protocols

**This Focus Area requires the following optional Knowledge Units:**

- Advanced Network Technology and Protocols
- Certification and Accreditation
- Intrusion Detection
- Life-Cycle Security
- Network Administration
- Network Forensics
- Penetration Testing
- Supply Chain Security
- Vulnerability Analysis

## Network Security Engineering

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the design of secure network infrastructures and security analysis of network traffic.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Scripting or Introductory Programming
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Network Defense
- Networking Technology and Protocols

**This Focus Area requires the following optional Knowledge Units:**

- Advanced Cryptography
- Advanced Network Technology and Protocols
- Analog Telecommunications
- Digital Communications
- Life-Cycle Security
- Mobile Technologies
- Network Administration
- Network Forensics
- Penetration Testing
- RF Principles
- Security Risk Analysis
- Supply Chain Security
- Systems Engineering
- Vulnerability Analysis

## Secure Cloud Computing

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the design, development, operation and maintenance of secure cloud architectures.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Scripting or Introductory Programming
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- Intro to Cryptography
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Network Defense
- Networking Technology and Protocols
- Operating Systems Concepts

**This Focus Area requires the following optional Knowledge Units:**

- Advanced Cryptography
- Advanced Network Technology and Protocols
- Cloud Computing
- IA Compliance
- Life-Cycle Security
- Network Administration
- Operating Systems Hardening
- Operating Systems Theory
- Security Risk Analysis
- Supply Chain Security
- Virtualization Technologies
- Vulnerability Analysis

## Secure Embedded Systems

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the design, development, analysis and secure use of embedded systems technologies.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Scripting or Introductory Programming
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Networking Technology and Protocols
- Operating Systems Concepts
- Programming

**This Focus Area requires the following optional Knowledge Units:**

- Data Structures
- Embedded Systems
- Hardware Reverse Engineering
- Hardware/Firmware Security
- Industrial Control Systems
- Life-Cycle Security
- Low Level Programming
- QA / Functional Testing
- Secure Programming Practices
- Supply Chain Security
- Systems Programming

## Secure Mobile Technology

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the secure design, development, utilization and management of mobile technologies, devices and services.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Networking Technology and Protocols

**This Focus Area requires the following optional Knowledge Units:**

- Advanced Network Technology and Protocols
- Data Structures
- Device Forensics
- Digital Communications
- Hardware/Firmware Security
- IA Compliance
- IA Standards
- Life-Cycle Security
- Mobile Technologies
- Network Forensics
- RF Principles
- Secure Programming Practices
- Security Risk Analysis
- Supply Chain Security
- Systems Programming
- Wireless Sensor Networks

## Secure Software Development

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the development of secure software (i.e., software that performs only it's intended functions without the presence of exploitable vulnerabilities).

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Scripting or Introductory Programming
- Fundamental Security Design Principles
- IT Systems Components

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Programming

**This Focus Area requires the following optional Knowledge Units:**

- Algorithms
- Data Structures
- Formal Methods
- Secure Programming Practices
- Software Assurance
- Software Security Analysis
- Vulnerability Analysis

## Secure Telecommunications

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the design, development and secure use of secure telecommunications systems, digital and analog.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Cyber Threats
- Fundamental Security Design Principles
- Intro to Cryptography
- Networking Concepts
- Policy, Legal, Ethics, and Compliance

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Network Defense
- Networking Technology and Protocols

**This Focus Area requires the following optional Knowledge Units:**

- Advanced Network Technology and Protocols
- Analog Telecommunications
- Digital Communications
- Life-Cycle Security
- Low Level Programming
- Mobile Technologies
- Network Administration
- Network Forensics
- RF Principles
- Security Risk Analysis
- Supply Chain Security
- Systems Engineering
- Systems Programming

## Security Incident Analysis and Response

This Focus Area encompasses the Knowledge Units 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.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Data Analysis
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Network Defense
- Networking Technology and Protocols
- Operating Systems Concepts

**This Focus Area requires the following optional Knowledge Units:**

- Cybersecurity Planning and Management
- Digital Investigations
- IA Architectures
- IA Compliance
- IA Standards
- Life-Cycle Security
- Operating Systems Hardening
- Overview of Cyber Operations
- Security Program Management
- Security Risk Analysis
- Supply Chain Security
- Vulnerability Analysis

## Security Policy Development and Compliance

This Focus Area encompasses the Knowledge Units 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.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- IT Systems Components
- Policy, Legal, Ethics, and Compliance
- System Administration

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- None

**This Focus Area requires the following optional Knowledge Units:**

- Cybersecurity Planning and Management
- IA Architectures
- IA Compliance
- IA Standards
- Life-Cycle Security
- Security Program Management
- Security Risk Analysis
- Supply Chain Security

## System Security Administration

This Focus Area encompasses the Knowledge Units necessary to impart the necessary skills and abilities for the secure configuration, operation and maintenance of a computer system (host or workstation).

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Scripting or Introductory Programming
- Cyber Defense
- Cyber Threats
- IA Fundamentals
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Network Defense
- Networking Technology and Protocols
- Operating Systems Concepts

**This Focus Area requires the following optional Knowledge Units:**

- Certification and Accreditation
- Host Forensics
- IA Architectures
- IA Compliance
- IA Standards
- Intrusion Detection
- Life-Cycle Security
- Network Administration
- Operating Systems Hardening
- Security Program Management
- Security Risk Analysis
- Supply Chain Security
- Systems Engineering
- Vulnerability Analysis

## Systems Security Engineering

This Focus Area encompasses the Knowledge Units 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.

**This Focus Area builds on the following 2-Year core Knowledge Units:**

- Basic Scripting or Introductory Programming
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance

**This Focus Area builds on the following 4-Year core Knowledge Units:**

- Networking Technology and Protocols
- Operating Systems Concepts

**This Focus Area requires the following optional Knowledge Units:**

- Advanced Network Technology and Protocols
- Cybersecurity Planning and Management
- Data Structures
- IA Architectures
- IA Standards
- Life-Cycle Security
- Low Level Programming
- Operating Systems Hardening
- QA / Functional Testing
- Security Risk Analysis
- Supply Chain Security
- Systems Engineering
- Systems Programming
- Virtualization Technologies