NSA/DHS National Centers of Academic Excellence in Information Assurance/Cyber Defense
2014 List of Knowledge Units and Focus Areas

The CAE IA/CD academic requirements are based on meeting defined sets of Knowledge Units (KUs):

1. **Core for 2 year programs** - *technical or applied emphasis*
2. **Core for 4 year+ programs** - *technical or applied emphasis*
3. **Optional KUs** - *4 year+ institutions must meet a minimum of five (5) optional KUs*[1]

1. CORE KUs for 2 year programs

- **1.1. Basic Data Analysis**
- **1.2. Basic Scripting or Introductory Programming (4 yr core)**
- **1.3. Cyber Defense**
- **1.4. Cyber Threats**
- **1.5. Fundamental Security Design Principles**
- **1.6. IA Fundamentals**
- **1.7. Intro to Cryptography**
- **1.8. IT Systems Components**
- **1.9. Networking Concepts**
- **1.10. Policy, Legal, Ethics, and Compliance**
- **1.11. System Administration**

2. CORE KUs for 4 year + programs

Includes all of the above 2 year core KUs **and:**

- **2.1. Databases**
- **2.2. Network Defense**
- **2.3. Networking Technology and Protocols**
- **2.4. Operating Systems Concepts**
- **2.5. Probability and Statistics**
- **2.6. Programming**

3. Optional KUs

- 3.1. Advanced Cryptography *(h,i,k)*[2]
- 3.2. Advanced Network Technology and Protocols *(g,h,i,m,q)*
- 3.3. Algorithms *(l)*
- 3.4. Analog Telecommunications *(h,m)*
- 3.5. Cloud Computing *(b,i)*
- 3.6. Cybersecurity Planning and Management *(b,f,n,o,p,q)*
- 3.7. Data Administration *(b,c,e)*
- 3.8. Data Structures *(d,j,k,l,q)*
- 3.9.Database Management Systems *(b,e)*
- 3.10. Digital Communications *(a,h,k,m)*
- 3.11. Digital Forensics *(n)*
- 3.12. Host Forensics *(d,p)*
- 3.13. Device Forensics *(d,k)*
- 3.14. Media Forensics *(d)*
- 3.15. Network Forensics *(d,g,h,k,m)*
- 3.16. Embedded Systems *(f,j)*
- 3.17. Forensic Accounting *(a,d)*
- 3.18. Formal Methods *(l)*
- 3.19. Fraud Prevention and Management *(a)*
- 3.20. Hardware Reverse Engineering *(d,j)*
- 3.21. Hardware/Firmware Security *(f,j,k)*
- 3.22. IA Architectures *(c,n,o,p,q)*
- 3.23. IA Compliance *(a,b,c,e,i,k,n,o,p)*
- 3.24. IA Standards *(e,k,n,o,p,q)*
- 3.25. Independent/Directed Study/Research
- 3.26. Industrial Control Systems *(f,j)*
- 3.27. Intro to Theory of Computation
- 3.28. Intrusion Detection *(c,f,g,p)*
- 3.29. Life-Cycle Security *(e,g,h,i,j,k,m,n,o,p,q)*
- 3.30. Low Level Programming *(j,m,q)*
- 3.31. Mobile Technologies *(h,k,m)*
- 3.32. Network Security Administration *(g,h,i,m,p)*
- 3.33. Operating Systems Hardening *(f,i,n,p,q)*
- 3.34. Operating Systems Theory *(d,i)*
- 3.35. Overview of Cyber Operations *(n)*
- 3.36. Penetration Testing *(g,h)*
- 3.37. QA / Functional Testing *(j,q)*
- 3.38. RF Principles *(h,k,m)*
- 3.39. Secure Programming Practices *(b,f,j,k,l)*
- 3.40. Security Program Management *(c,e,n,o,p)*
- 3.41. Security Risk Analysis *(a,b,c,f,h,i,k,m,n,o,p,q)*
- 3.42. Software Assurance *(l)*
- 3.43. Software Reverse Engineering *(d)*
- 3.44. Software Security Analysis *(e,l)*
- 3.45. Supply Chain Security *(e,g,h,i,j,k,m,n,o,p,q)*
- 3.46. Systems Programming *(j,k,m,q)*
- 3.47. Systems Certification and Accreditation *(g,p)*
- 3.48. Systems Security Engineering *(c,f,h,m,p,q)*
- 3.49. Virtualization Technologies *(q)*
- 3.50. Vulnerability Analysis *(d,f,g,h,i,l,n,p)*
- 3.51. Wireless Sensor Networks *(c,k)*

[1] Optional KUs are not required for CAE 2 year designation.

[2] *(h,i,k,etc)* = corresponding Focus Area on page 2

Each KU is composed of:

1. A minimum list of required topics to be covered
2. One or more "outcomes" or learning objectives

Applicants can use a variety of materials to meet/fulfill a KU to include:

- Course Syllabus
- Prerequisite Course(s)
- Prerequisite Degree
- Student Assignments
- Modules in a course/collection of courses
- Certifications (CCNA, etc)

(One course may fulfill the requirements of multiple KUs.)

---

4. FOCUS AREAS (Optional)

Applicants also have the option to apply for one or more "Focus Area" designations for their programs. A student must be able to complete the necessary course of study for that focus area. Each of the following focus areas is comprised of a subset of the KUs listed above:

a. Cyber Investigations
b. Data Management Systems Security
c. Data Security Analysis
d. Digital Forensics
e. Health Care Security
f. Industrial Control Systems-SCADA Security
g. Network Security Administration
h. Network Security Engineering
i. Secure Cloud Computing
j. Secure Embedded Systems
k. Secure Mobile Technology
l. Secure Software Development
m. Secure Telecommunications
n. Security Incident Analysis and Response
o. Security Policy Development and Compliance
p. Systems Security Administration
q. Systems Security Engineering

a. 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 exfiltrated, and residual effects

1.1. Basic Data Analysis
1.4. Cyber Threats
1.5. IA Fundamentals
1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
3.10. Digital Investigations

3.17. Forensic Accounting
3.19. Fraud Prevention and Management
3.23. IA Compliance
3.41. Security Risk Analysis

Back to Focus Area List

b. 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

1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals
1.7. Intro to Cryptography
1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
1.11. System Administration
2.1. Databases
2.4. Operating Systems Concepts
3.5. Cloud Computing
3.6. Cybersecurity Planning and Management
3.7. Data Administration
3.9. Database Management Systems
3.23. IA Compliance
3.39. Secure Programming Practices
3.41 Security Risk Analysis

Back to Focus Area List

c. 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

1.1. Basic Data Analysis
1.2. Basic Scripting or Introductory Programming
1.5. Fundamental Security Design Principles
1.9. Networking Concepts
2.1. Databases
2.5. Probability and Statistics
3.7. Data Administration
3.22. IA Architectures
3.23. IA Compliance
3.28. Intrusion Detection
3.40. Security Program Management
3.41. Security Risk Analysis
3.48. Systems Security Engineering
3.51. Wireless Sensor Networks

Back to Focus Area List

d. 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

1.2. Basic Scripting or Introductory Programming
1.6. IA Fundamentals
1.7. Intro to Cryptography
1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
1.11. System Administration
2.3. Networking Technologies and Protocols
2.4. Operating Systems Concepts
3.8. Data Structures
3.12. Host Forensics
3.13. Device Forensics
3.14. Media Forensics
3.15. Network Forensics
3.17. Forensic Accounting
3.20. Hardware Reverse Engineering
3.34. Operating Systems Theory
3.43. Software Reverse Engineering
3.50. Vulnerability Analysis

Back to Focus Area List

e. Healthcare 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

1.3. Cyber Defense
1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals
1.7. Intro to Cryptography
1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
1.11. System Administration
2.1. Databases
2.2. Network Defense
3.7. Data Administration
3.9. Database Management Systems
3.23. IA Compliance
3.24. IA Standards
3.29. Life-Cycle Security
3.40. Security Program Management
3.44. Software Security Analysis
3.45 Supply Chain Security

Back to Focus Area List

f. 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)

1.3. Cyber Defense
1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals
1.8. IT Systems Components
1.9. Networking Concepts
1.11. System Administration
2.2. Network Defense
2.3. Networking Technology and Protocols
2.4. Operating Systems Concepts
3.6. Cybersecurity Planning and Management
3.16. Embedded Systems
3.21. Hardware/Firmware Security
3.26. Industrial Control Systems
3.28. Intrusion Detection
3.33. Operating Systems Hardening
3.39. Secure Programming Practices
3.41. Security Risk Analysis
3.48. Systems Security Engineering
3.50. Vulnerability Analysis

Back to Focus Area List

g. 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)

1.2. Basic Scripting or Introductory Programming
1.4. Cyber Threats
1.6. IA Fundamentals
1.7. Intro to Cryptography
1.8. IT Systems Components
1.9. Networking Concepts
2.2. Network Defense
2.3. Networking Technology and Protocols
3.2. Advanced Networking Technology and Protocols
3.15. Network Forensics
3.28. Intrusion Detection
3.29. Life-Cycle Security
3.32. Network Security Administration
3.36. Penetration Testing
3.45. Supply Chain Security
3.47. Systems Certification and Accreditation

3.50. Vulnerability Analysis

Back to Focus Area List

h. 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

1.2. Basic Scripting or Introductory Programming
1.3. Cyber Defense
1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals
1.7. Intro to Cryptography
1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
2.2. Network Defense
2.3. Networking Technology and Protocols
3.1 Advanced Cryptography
3.2. Advanced Networking Technology and Protocols
3.4. Analog Telecommunications
3.10. Digital Communications
3.15. Network Forensics
3.29. Life-Cycle Security
3.31. Mobile Technologies
3.32. Network Security Administration
3.36. Penetration Testing
3.38. RF Principles
3.41. Security Risk Analysis
3.45. Supply Chain Security
3.48. Systems Security Engineering
3.50. Vulnerability Analysis

Back to Focus Area List

i. Secure Cloud Computing

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

1.2. Basic Scripting or Introductory Programming
1.3. Cyber Defense
1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals
1.7. Intro to Cryptography
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
1.11. System Administration
2.2. Network Defense
2.3. Networking Technology and Protocols
2.4. Operating Systems Concepts

3.1 Advanced Cryptography
3.2. Advanced Networking Technology and Protocols
3.5. Cloud Computing
3.23. IA Compliance
3.29. Life-Cycle Security
3.32. Network Security Administration
3.33. Operating Systems Hardening
3.34. Operating Systems Theory
3.41. Security Risk Analysis
3.45. Supply Chain Security
3.49. Virtualization Technologies
3.50. Vulnerability Analysis

Back to Focus Area List

j. Secure Embedded Systems

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

1.2. Basic Scripting or Introductory Programming
1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals
1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
2.3. Networking Technology and Protocols
2.4. Operating Systems Concepts
2.6. Programming
3.8. Data Structures
3.16. Embedded Systems
3.20. Hardware Reverse Engineering
3.21. Hardware/Firmware Security
3.26. Industrial Control Systems
3.29. Life-Cycle Security
3.30. Low Level Programming
3.37. QA/Functional Testing
3.39. Secure Programming Practices
3.45. Supply Chain Security
3.46. Systems Programming

Back to Focus Area List

k. 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

1.3. Cyber Defense
1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals

1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
2.3. Networking Technology and Protocols
3.2. Advanced Networking Technology and Protocols
3.8. Data Structures
3.10 Digital Communications
3.13. Device Forensics
3.15. Network Forensics
3.21. Hardware/Firmware Security
3.23. IA Compliance
3.24. IA Standards
3.29. Life-Cycle Security
3.31. Mobile Technologies
3.38. RF Principles
3.39. Secure Programming Practices
3.41. Security Risk Analysis
3.45. Supply Chain Security
3.46. Systems Programming
3.51. Wireless Sensor Networks

Back to Focus Area List

l. 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)

1.2. Basic Scripting or Introductory Programming
1.5. Fundamental Security Design Principles
1.8. IT Systems Components
2.6. Programming
3.3. Algorithms
3.8. Data Structures
3.18. Formal Methods
3.39. Secure Programming Practices
3.42. Software Assurance
3.44. Software Security Analysis
3.50. Vulnerability Analysis

Back to Focus Area List

m. 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

1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.7. Intro to Cryptography
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
2.2. Network Defense

2.3. Networking Technology and Protocols
3.2. Advanced Networking Technology and Protocols
3.4. Analog Communications
3.10. Digital Communications
3.15. Network Forensics
3.29. Life-Cycle Security
3.30. Low Level Programming
3.31. Mobile Technologies
3.32. Network Security Administration
3.38. RF Principles
3.41. Security Risk Analysis
3.45. Supply Chain Security
3.46. Systems Programming
3.48. Systems Security Engineering

Back to Focus Area List

n. 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

1.1. Basic Data Analysis
1.3. Cyber Defense
1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals
1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
1.11. System Administration
2.2. Network Defense
2.3. Networking Technology and Protocols
2.4. Operating Systems Concepts
3.6. Cybersecurity Planning and Management
3.11. Digital Forensics
3.22. IA Architectures
3.23. IA Compliance
3.24. IA Standards
3.29. Life-Cycle Security
3.33. Operating Systems Hardening
3.35. Overview of Cyber Operation
3.40. Security Program Management
3.41. Security Risk Analysis
3.45. Supply Chain Security
3.50. Vulnerability Analysis

Back to Focus Area List

o. 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

1.3. Cyber Defense
1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals
1.8. IT Systems Components
1.10. Policy, Legal, Ethics, and Compliance
1.11. System Administration
3.6. Cybersecurity Planning and Management
3.22. IA Architectures
3.23. IA Compliance
3.24. IA Standards
3.29. Life-Cycle Security
3.40. Security Program Management
3.41. Security Risk Analysis
3.45. Supply Chain Security

Back to Focus Area List

p. 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)

1.2. Basic Scripting or Introductory Programming
1.3. Cyber Defense
1.4. Cyber Threats
1.6. IA Fundamentals
1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
1.11. System Administration
2.2. Network Defense
2.3. Networking Technology and Protocols
2.4. Operating Systems Concepts
3.6. Cybersecurity Planning and Management
3.12. Host Forensics
3.22. IA Architectures
3.23. IA Compliance
3.24. IA Standards
3.28. Intrusion Detection
3.29. Life-Cycle Security
3.32. Network Security Administration
3.33. Operating Systems Hardening
3.40. Security Program Management
3.41. Security Risk Analysis
3.45. Supply Chain Security
3.47. Systems Certification and Accreditation

3.48. Systems Security Engineering
3.50. Vulnerability Analysis

Back to Focus Area List

q. System 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

1.2. Basic Scripting or Introductory Programming
1.3. Cyber Defense
1.4. Cyber Threats
1.5. Fundamental Security Design Principles
1.6. IA Fundamentals
1.8. IT Systems Components
1.9. Networking Concepts
1.10. Policy, Legal, Ethics, and Compliance
2.3. Networking Technology and Protocols
2.4. Operating Systems Concepts
3.2. Advanced Networking Technology and Protocols
3.6. Cybersecurity Planning and Management
3.8. Data Structures
3.22. IA Architectures
3.24. IA Standards
3.29. Life-Cycle Security
3.30. Low Level Programming
3.33. Operating Systems Hardening
3.37. QA/Functional Testing
3.41. Security Risk Analysis
3.45. Supply Chain Security
3.46. Systems Programming
3.48. Systems Security Engineering
3.49. Virtualization Technologies