Center of Academic Excellence – Cyber Operations Program | 2013 Application

Name of Institution:

Date:

Mailing Address of Institution:

Institution's President's Name and Official Email Address:

Department Submitting Application (e.g., Computer Science (CS), Electrical Computing Engineering (ECE), etc.):

Applying at which program level: **Undergraduate** ○ **Graduate*** ○ **Both** ○
(* See question #2 below)

<u>Accreditations</u>

Nationally accredited?
Yes ○
No ○

Regionally accredited?
Yes ○
No ○

Name of National Accreditation Body:

Name of Regional Accreditation Body:

Date of National Accreditation:

Date of Regional Accreditation:

<u>Institution's Points of Contact (POC)</u>

***Primary* POC Name:**

Office Phone #:

Office Email Address:

***Alternate* POC #1 Name:**

Office Phone #:

Office Email Address:

Alternate POC #2 Name: **Alternate POC #3 Name:**

Office Phone # and Official Email Address: **Office Phone # and Official Email Address:**

1. **Identify courses believed to cover the academic requirements knowledge units in the knowledge unit alignment worksheet** ***(see Criteria 1 and 5)****. If applying at the graduate* ***and*** *undergraduate level, please* ***complete separate KU alignment worksheets for the graduate and undergraduate programs****. If graduate courses may be taken by undergraduate students, those courses may be included in the undergraduate matrix.*

NOTE: this portion is completed by filling out the Knowledge Unit Alignment Worksheet. Any additional comments referencing the worksheet may be placed here.

2. **Identify the Degree Program(s) in which the Cyber Operations curriculum is based and include the title of the degree/specialization/track, sample course schedule, course description and syllabi that contain a weekly schedule of topics.** *Please note-- if applying at the graduate level and enrolling students are expected to have already met some of the CAE Cyber Operations mandatory requirements, indicate how students may demonstrate that those requirements are met.*

3. **Describe how students who participate in the Cyber Operations curricula will be distinguished from other (non-Cyber Operations) students *(see Criteria 2)*:**

4. **Provide a list of research topics believed to be related to the Cyber Operations Program in which faculty are currently involved *(See Criteria 6)*:**

5. **Provide research topics believed to be related to the Cyber Operations Program in which students are currently engaged or could engage *(See Criteria 7)*:**

6. **Describe Cyber Operations-related outreach efforts in which students are currently involved or could participate (e.g., Cyber exercises, volunteers at local K-12 schools, cyber camps, etc.) *(See Criteria 8)*:**

7. **Identify the names and number of faculty who teach active Cyber Operations-related program courses *(See Criteria 10)*:**

<u>Continuation and Additional Comments:</u>

Our Institution understands and believes that our program meets the criteria defined for the CAE-Cyber Operations program and has active courses that cover the mandatory knowledge units and at least 60 percent of the optional units to meet the academic content requirements. Our Institution agrees, as part of the application process, that its program will participate in an in-person curricula review of courses satisfying the mandatory and optional knowledge units as part of the application review and selection process. If designated as a CAE-Cyber Operations Institution, our institution agrees to participate in NSA-hosted Summer Seminars as part of the program *(See Criteria 9)*.

_________________________________ **______________________**

Signature **Date**

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:

MANDATORY KNOWLEDGE UNITS	Course #	Course Title	Date Last Taught	Date Last Updated
Low Level Programming				
C				
Write a program that implements a network stack to manage network comms				
Assembly				
Write a functional, stand-alone assembly language programmimplementing a basic telnet client (no help)				
Develop programs that can be embedded in OS kernel				
Implement exploits for discovered vulnerabilties				
Reverse Engineering				
Malware Analysis				
Reverse Engineering tools				
Communications (including protocols)				
Software				
Use of IDAPro				
Safely perform static & dynamic analysis				
Use a tool to safely perform static and dynamic analysis (malware) of unknown origin				
Covers appropriate tools, techniques & procedures				
Operating System Theory				
Privileged vs non-privileged states				
Concurrency and synchronization				

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:				
Processes and threads, process/thread mgt, inter-process comms				
Memory mgt/virtual memory				
File Systems				
IO Issues (buffering, queuing, sharing, mgt)				
Disributed OS issues (client/server, message passing, etc.)				
Understand OS internals to the level that they could design & implement significant architectural changes to an existing OS				
Networking				
TCP/IP				
Protocols (routing network & application protocols)				
Architectures				
Wireless				
Traffic Analysis				
Protocol Analysis				
Know how networks transfer data				
Know how to enable communications				
Know how the lower network layers support the upper ones				
Telecommunications				
Mobile				
Telephony				
Insfrastructures (i.e., fiber otpic network)				
Core Network (Mobile and Inernet)				
Describe routing in a telecomm network				

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:				
Describe interaction of elements w/in the telecomm core				
Describe end-to-end delivery of a packet and/or signal				
Understand what happnes with the hand-off at each step along the way				
Explain differences in core architecture btwn different generations of mobile network technology				
Discrete Math				
Introduce 1st order logic graphs, accounting, accountability, and induction proofs.				
Algorithms				
Exposed to fundamental algorithm sorting/searching/data/manipulation				
Analyze the complexity of algorithms				
Statistics/Calculus I & II				
Understand how variability affects outcomes				
How to identify anamolous events				
How to identify the meaing of anamolous events				
Able to integrate and differentiate continuous functions of multiple variables				
Automota				
Understand how automota is used to describe computing machines & computation & notion that some things are computable and some are not				
Understand the connection btwn automata and computer languages				
Describe the hiearchy of language from regular expression to context files				

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:

Legal				
Laws, Regulations, Directives, and Policies				
Understand the legal issues governing the authorized conduct of cyber operations and use of related tools, techniques, technology, and data				
Overview of Cyber Defense (incl. hands-on labs/exercises)				
Network Security Techniques and Components (e.g., Firewalls, IDS, etc.)				
Cryptography (include PKI Cryptography)				
Malicious Activity Detection				
Identification of reconnaissance operations				
Anomaly/Intrusion detection				
Anomaly identification				
Identification of command and control operations				
Identifying malicious code based on signatures, behavior and artifacts System Security Archit.				
Defense in depth Trust Relationships				
Distributed/Cloud				
Virtualization				
Describe, evaluate, and operate defense network architecture employing multiple layers of protection using technology appropriate for secure misssion accomplishment				

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:

Security Fundamental Principles (1st Principles of				
Domain Separation				
Process Isolation				
Resource Encapsulation				
Least Privilege				
Layering/Abstraction/Data Hiding				
Modularity/Minimization				
Security Policies				
Applied Cryptography				
Understand fundamental principles underlying cyber security				
How these principles inter-relate and are typically employed to achieved assured solutions				
Vulnerabilities				
Vulnerability Taxonomy Root Causes Buffer Overflows Privilege Escalation Attacks				
Trojans/Backdoors/Viruses				
Rootkits				
Understand the various types of vulnerabilities, their underlying causes, and the ways in which they were exploited				
Know how to avoid these vulnerabilities during system design, development, and implementation				

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:

OPTIONAL KNOWLEDGE UNITS	Course #	Course Title	Date Last Taught	Date Last Updated
Programmable Logic Languages				
FPGA Design				
Albe to specify digital device behavior using a programmable logic language				
Wireless Security				
Describe the unique security and operational attributes in the wireless environment and their effects on network communications				
Identify the unique security implications of these effects and how to mitigate security issues associated with them				
Virtualization				
Discuss the advantages and disadvantages of virtualization				
Identify the different approaches for virtualizing computer systems and the security implications of each different approach				
Large Scale Distributed Systems				
Cloud computing/Cloud security				
Describe different kinds of Cloud architecture models, services, security issues, and components (logical and physical)				
Identify all associated data paths within a given cloud design				
Risk Managmenet of Information Systems				

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:

Identify classes of possible threats, what are the consequences associated with each threat, and what actions can be taken to mitigate the threat				
Computer Architecture				
Define devices of electronic digital circuits and describe how these components are interconnected				
Integrate individual components into a more complex digital system and understand the data path through a CPU.				
Microcontroller Design				
Integrate discrete components into a single processor element and describe ways of achieving performance efficiencies through combining components.				
Identify trade-offs associated with microcontroller optimization.				
Software Analysis				
System Source Code				
Static and Dynamic Techniques				
Testing (Black box/White box/Fuzz)				
Perform analysis of existing source code for functional correctness.				
Apply industry standard tools that analyze software for security vulnerabilities.				
Through the application of testing methodologies, students should be able to build test cases that demonstrate the existence of vulnerabilities.				

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:				
Secure Software Development (Building secure software)				
Secure Programming Principles and Practices				
Constructive Techniques				
Demonstrate that they understand the techniques specifying program behavior, the classes of well known defects.				
How they manifest themselves in various languages and are capable of authoring programs that are free from defects.				
Embedded Systems				
Define requirements which lead to the design and fabrication of an embedded system.				
Program the microcontrollers to achieve an application specific design and identify the security concerns associated with resource-constrained devices.				
Forensics				
Operating Systems				
Network Forensics				
Determine the manner in which an operating system or application has been subverted, recover “deleted” and/or intentionally hidden information from various types of media and demonstrate proficiency with handling of a large number of different kinds of components.				
Secure Systems Programming				
Kernel Internals				

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:				
Device Drivers				
Multi-Threading				
Use of alternate processors				
Build and integrate kernel modules, understand the system call mechanism and how malicious software subverts system calls.				
Demonstrate sufficient knowledge of the networking stack to be able to construct network filter components.				
Discuss strengths and weaknesses of alternative processors, demonstrate familiarity of toolsets for making use of alternative processors (e.g., GPUs).				
Applied Cryptography				
Identify the appropriate uses of symmetric and asymmetric encryption.				
Assign some measure of strength to cryptographic algorithms and the associated keys.				
Identify what level of algorithm strength is needed for particular applications and the implementation factors related to its suitability for use.				
Understand the common pitfalls associated with the implementation of cryptography.				
Understand the challenges and limitations of various key management systems.				
SCADA Systems				
Describe how embedded systems are employed in industrial infrastructures and control systems.				
Describe methods for management of distributed nodes				

CAE-CYBER OPERATIONS PROGRAM
COURSE ALIGNMENT TO KNOWLEDGE UNITS

Institution Name:				
Identify potential security vulnerabilities associated with the use of such systems and means for mitigating these vulnerabilities.				
HCI/Usable Security				
Understand user interface issues that will affect the implementation of and perception of security mechanisms and the behavioral impacts of various security "policies".				
Understand the tension between user security and convenience.				