CAE Mapping Approach

Fred Klappenberger
National CyberWatch Center

Review - Mapping

- New NSA/DHS requirements

- 75 Knowledge Units replace 6 CNSS standards
  - KUs - targeted technology areas composed of Topics and expected Outcomes
  - 3 KU categories: Core, Mandatory, and Optional

Mapping in Brief

Knowledge Units

Ways to demonstrate that a program meets/fulfills a Knowledge Unit

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

A course may fulfill the requirements of multiple Knowledge Units.

From: https://www.iad.gov/NIETP/documents/Requirements/CAE_IA-CD_KU.pdf

KU Breakdown & Minimum Rqmts

- Core 2Y: 11 Mandatory KUs
  - 2 year institutions must map to all 11
- Core 4Y: 17 Mandatory KUs
  - 4 year institutions must map additional 6
- Optional KUs: 53 Elective KUs
  - 4 year institutions must select 5

- ***Summary of Minimums: 2Y – 11 KUs; 4Y – 22 KUs***

Mapping Resources

- Course Materials: syllabi, detailed course outlines, textbooks, lab exercises, handouts, ...
- KUs - download Reference Materials at
  http://www.cisse.info/news/cae-certification or
  https://www.iad.gov/NIETP/CAERequirements.cfm
- Content Experts: faculty who teach topics

Sample Mapping Resource

Detailed Course Outline:

Dates Mon	Dates Wed	Topics and Assigned Readings
	1/8	Course introduction, assign User ID, discuss passwords. What is shell scripting? Why is it important to know? POSIX and portability. File, directory, and pathname concept review. Review basic commands: `cd`, `pwd`, `pathchk`, `mkdir`, `rmdir`, `passwd`, `cp`, `mv`, `rm`, `ln`, `ls -laRd`, `who`, `echo`, `cat`, `more` and `less`, `tac` and `rev`. Useful non-standard utilities include: `pwgen` and `apg`, `script` and `screen`, and `readlink`. Using `man`, `info`, and other resources. **Readings:** Chapters 1, 2, Appendix B, man pages for listed commands
1/13	1/15	The `vi` and `vim` (and other) text editors. **Readings:** online vi/vim resources, (Chapter 22 in Hahn)
1/20		**Martin Luther King Jr. Day — HCC Closed**
1/22	1/27	Shell features: *globbing* (wildcards), *locales* (I18N), I/O redirection, pipelines. Using `here` documents. Understanding processes, process groups (jobs), and sessions. Project 1 due: 1/22 **Readings:** Chapters 2 (pages 24–38), 3, 295-297, 352-360, on-line locale resources, (465-471 in Hahn book)
1/29	2/3 2/5	Regular Expressions (BREs, EREs, PREs, and POSIX). Some common filter commands: `sed`, `cut`, `paste`, `tr`, `tail` (also `tailf` and `head`), `wc`, `grep`, `sort`, `uniq`, `od` and `xxd`, `strings`, `diff` (and `cmp`, `vimdiff` `sdiff`, `comm`, and `patch`), `yes`, `nl`, and XML utilities (`xmlgrep`, `xmldiff`, and others). Project 2 due: 2/3 **Readings:** Chapter 4, on-line *regular expression* resources
2/10		**Exam #1**
2/12		Python basics: variables, statements, if-statements, loops, ...

Sample Mapping Resource

Syllabus Course Objectives:

- Describe gaining confidential information or unauthorized access through human intelligence (i.e. social engineering)
- Discuss counter measures to social engineering (training and education of users, administrators and personnel)
- Describe phishing
- Define organizational policies and procedures
- Describe security policies (guidance provided by security policies, points of contact, roles and responsibilities, enterprise, issue specific, and system specific security policies)
- Describe AIS and telecommunications systems policies (points of contact, references)
- Explain change management
- Explain classification of information
- Describe documentation, logs, and journals
- Explain acceptable use of resources, internet usage policy, and e-mail usage policy
- Discuss due care, due diligence, and due process
- Describe separation of duties, need to know and least privilege
- Discuss transportation of media
- Explain monitoring of critical areas, communications centers, information systems centers (IT/data centers), protected distributed systems, stand-alone systems, peripherals, storage areas
- Describe Policies and Procedures for computers and users
- etc.

Sample Mapping Resource

Network Security Fundamentals
COMSEC 215
Fall Term, 2014

Week	Topics	Chapter Readings	Labs & *Exams*
1	**Introduction to Security** • Challenges of securing information • Importance of information security • Types of attackers – hackers, script kiddies, spies, insiders • Attack types and defenses - 5 basic principles of defense	Chapter 1	Review lab procedures Scan for malware *End of Chapter questions*
2	**Malware and Social Engineering Attacks** • Types of malware • Worms, trojans, rootkits, backdoors, botnets, spyware, adware, keyloggers • Social Engineering – psychological, phishing, impersonation, spam, hoaxes • Physical – dumpster diving, tailgating,	Chapter 2	USB blocking Rootkit scanning Sw keylogger *End of Chapter questions*
3	**Application and Network Attacks** • XSS, SQL and SML injection • Cookies, attachments, hijacking, malicious add-ons, DoS, buffer overflows, man-in-the-middle, replay, ARP and DNS poisoning, privilege escalation	Chapter 3	***Quiz Ch 1 & 2*** Browser security Create HTTP header *End of Chapter questions*
4	**Vulnerability Assessment and Mitigating Attacks** • Identify assets, evaluate threats, appraise vulnerability, assess & mitigate risk • Baseline, sw program development	Chapter 4	Port Scanning Penetration tests
5	**Host, Application, and Data Security** • Physical, hardware, mobile device, OS security • Baselining • Anti-malware, firewalls, logs • Applications, secure coding, hardening, patching • Securing data	Chapter 5	***Quiz Ch 3 & 4*** Setting firewalls MS Event Viewer *End of Chapter questions*

Sample Mapping Resource

Network Security Fundamentals
COMSEC 215
Fall Term, 201_

Week	Topics	Chapter Readings	Labs & *Exams*
1	**Introduction to Security** 1. Challenges of securing information 2. Importance of information security 3. Types of attackers – hackers, script kiddies, spies, insiders 4. Attack types and defenses - 5 basic principles of defense	Chapter 1	L1 Review lab procedures L2 Scan for malware R1 *End of Chapter questions*
2	**Malware and Social Engineering Attacks** 1. Types of malware 2. Worms, trojans, rootkits, backdoors, botnets, spyware, adware, keyloggers 3. Social Engineering – psychological, phishing, impersonation, spam, hoaxes 4. Physical – dumpster diving, tailgating,	Chapter 2	L3 USB blocking L4 Rootkit scanning L5 Sw keylogger R2 *End of Chapter questions*
3	**Application and Network Attacks** 1. XSS, SQL and SML injection 2. Cookies, attachments, hijacking, malicious add-ons, DoS, buffer overflows, man-in-the-middle, replay, ARP and DNS poisoning, privilege escalation	Chapter 3	*Quiz Ch 1 & 2* L6 Browser security L7 Create HTTP header R3 *End of Chapter questions*
4	**Vulnerability Assessment and Mitigating Attacks** 1. Identify assets, evaluate threats, appraise vulnerability, assess & mitigate risk 2. Baseline, sw program development	Chapter 4	L8 Port Scanning L9 Penetration tests R4 *End of Chapter questions*
5	**Host, Application, and Data Security** 1. Physical, hardware, mobile device, OS security 2. Baselining 3. Anti-malware, firewalls, logs 4. Applications, secure coding, hardening, patching 5. Securing data	Chapter 5	*Quiz Ch 3 & 4* L10 Setting firewalls L11 MS Event Viewer R5 *End of Chapter questions*

Sample Mapping Resource

DETAILED COURSE OUTLINE

Main Topic		Lecture Hours
1.0	Introduction to Operating Systems (DOS, Windows, Unix/Linux)	3.0
	1.1 Hardware and Terminal Components	
	1.2 System startup	
	1.3 Command Syntax and Execution	
	1.4 File Names, Extensions, Wild Card Characters	
	1.5 Default Drives and Directories	
	1.6 System Prompts	
	1.7 Getting Help with Command Information	
	1.8 Restarting the System	
	1.9 Shutting Down the System	
2.0	Disk Preparation and File Management Commands (DOS, Windows, Unix/Linux)	2.0
	2.1 Floppy Disk Utilities	
	2.2 Disk Format Operations and Partitioning	
	2.3 File Commands and Disk Navigation	
3.0	Directory Management Commands (DOS, Windows, Unix/Linux)	2.0
	3.1 Common Directories and Subdirectories	
	3.2 Creating and Removing Subdirectories	
4.0	Common System Utilities (DOS, Windows, Unix/Linux)	4.0
	4.1 Disk Space Management	
	4.2 Other File Commands	
5.0	Creating and Editing ASCII/Text Files (DOS, Windows, Unix/Linux)	3.0
6.0	Data System Security and Device Control	2.0
	6.1 Backup and Restore Operations	
	6.2 Device Controls	

Sample Mapping Resource

Network Security Fundamentals
Objectives - Outcomes

Chapter/Week 1
OBJ 1.1 Describe the challenges of securing information
OBJ 1.2 Define information security and explain why it is important
OBJ 1.3 Identify the types of attackers that are common today
OBJ 1.4 List the basic steps of an attack
OBJ 1.5 Describe the five basic principles of defense

Chapter/Week 2
OBJ 2.1 Describe the differences between a virus and a worm
OBJ 2.2 List the types of malware that conceals its appearance
OBJ 2.3 Identify different kinds of malware that is designed for profit
OBJ 2.4 Describe the types of social engineering psychological attacks
OBJ 2.5 Explain physical social engineering attacks

Chapter/Week 3
OBJ 3.1 List and explain the different types of Web application attacks
OBJ 3.2 Define client-side attacks
OBJ 3.3 Explain how a buffer overflow attack works
OBJ 3.4 List different types of denial of service attacks
OBJ 3.5 Describe interception and poisoning attacks

Chapter/Week 4
OBJ 4.1 Define vulnerability assessment and explain why it is important
OBJ 4.2 List vulnerability assessment techniques and tools
OBJ 4.3Explain the differences between vulnerability scanning and penetration testing
OBJ 4.4 List techniques for mitigating and deterring attacks

Chapter/Week 5
OBJ 5.1 List the steps for securing a host computer
OBJ 5.2 Define application security
OBJ 5.3 Explain how to secure data using loss prevention

Detailed Course Outline

Suggestions to expedite mapping:

- Show weekly chronology of topics
- List topics and subtopics
- Show schedule of labs, reports, presentations, group projects, etc.
- Stipulate objectives and expected outcomes
- Show exam schedule and material
- Enumerate all above elements to simplify mapping references

Mapping - Three Steps

1. Offline Phase:
   - Identifying KUs that are to be mapped
   - Gathering and recording supporting course data
2. Online Phase:
   - Enter all courses (topics & objectives) into database
3. Online Phase:
   - Match courses to KU requirements

"I was floating in a tunnel toward a very bright light and then a voice told me I had to go back and finish listening to the presentation."

Phase I – Offline Data Gathering

Next series of slides provides a step-by-step procedure for collecting/organizing institutional course data

KU Mapping Matrix - Main Screen
(2014 CAE KU Mapping Matrix.ppt)

Click on name to jump to that KU

	A	B	C	D	E
1	All links below take you to the datasheet for that KU.				
2	**Core 2Y Knowledge Units**		**Optional Knowledge Units**		
3		Basic Data Analysis	Advanced Cryptography	Hardware Reverse Engineering	Secure Programming Practices
4		Basic Scripting	Advanced Network Technology and Protocols	Hardware/Firmware Security	Security Program Management
5		Cyber Defense	Algorithms	IA Architectures	Security Risk Analysis
6		Cyber Threats	Analog Telecommunications	IA Compliance	Software Assurance
7		Fundamental Security Design Principles	Cloud Computing	IA Standards	Software Reverse Engineering
8		Information Assurance Fundamentals	Cybersecurity Planning and Management	Independent/Directed Study/Research	Software Security Analysis
9		Introduction to Cryptography	Data Administration	Industrial Control Systems	Supply Chain Security
10		Information Technology System Components	Data Structures	Intro to Theory of Computation	Systems Programming
11		Networking Concepts	Database Management Systems	Intrusion Detection	Systems Certification and Accreditation
12		Policy. Legal, Ethics and Compliance	Digital Communications	Life-Cycle Security	Systems Security Engineering
13		Systems Administration	Digital Forensics	Low Level Programming	Virtualization Technologies
14			Device Forensics	Mobile Technologies	Vulnerability Analysis
15	**Core 4Y Knowledge Units**		Host Forensics	Network Security Administration	Wireless Sensor Networks
16		Databases	Media Forensics	Operating Systems Hardening	
17		Network Defense	Network Forensics	Operating Systems Theory	
18		Network Technology and Protocols	Embedded Systems	Overview of Cyber Operations	
19		Operating Systems Concepts	Forensic Accounting	Penetration Testing	
20		Probability and Statistics	Formal Methods	QA / Functional Testing	
21		Programming	Fraud Prevention and Management	RF Principles	

Structure of KUs

Basic features of all KUs:

Topics - Outcomes - Courses

	A	B	C	D	E
1				Courses ABC-123	DEF-456
2	Click here to return to KU Listing			(Click Here) READ	
3	**Basic Data Analysis**				
4		Provide students with basic abilities to manipulate data into meaningful information.			
5		**Topics**			
6			Summary statistics		
7			Graphing/Charts		
8			Spreadsheet Functions		
9			Problem Solving		
10		**Outcomes**			
11		Students will be able to:			
12			Apply standard statistical inference procedures to draw conclusions from data		

	A	B	C	D	E
1				ABC-123	DEF-456
2	Click here to return to KU Listing			(Click Here) READ	
3	**Basic Scripting**				
4		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).			
5		**Topics**			
6			*Basic Security		
7			Bounds checking, input validation		
8			Program Commands		
9			Program Control Structures		
10			Variable Declaration		
11			Debugging		
12			Scripting Language (e.g. PERL, Python, BASH, VB Scripting, Powershell)		
13			*Basic Boolean logic/operations		
14			AND / OR / XOR / NOT		
15		**Outcomes**			
16		Students will be able to:			
17			Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks)		
18			Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL)		
19			Write simple linear and looping scripts		

1st Time Mappers - Initial Course Identification

	A	B	C	D	E
1			Courses	MAT 135	CIS 210
2	Click here to return to KU Listing			(Click Here) REA	
3	**Basic Data Analysis**				
4		Provide students with basic abilities to manipulate data into meaningful information.			
5		**Topics**			
6			Summary statistics	X	
7			Graphing/Charts	X	
8			Spreadsheet Functions	X	
9			Problem Solving	X	X
10		**Outcomes**			
11		Students will be able to:			
12			Apply standard statistical inference procedures to draw conclusions from data	X	

	A	B	C	D	E
1			Courses	MAT 135	CIS 210
2	Click here to return to KU Listing				(Click H
3	**Basic Scripting**				
4		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).			
5		**Topics**			
6			*Basic Security		
7			Bounds checking, input validation		X
8			Program Commands		X
9			Program Control Structures		X
10			Variable Declaration		X
11			Debugging		X
12			Scripting Language (e.g. PERL, Python, BASH, VB Scripting,		X
13			*Basic Boolean logic/operations		
14			AND / OR / XOR / NOT		X
15		**Outcomes**			
16		Students will be able to:			
17			Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks)		X
18			Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL)		X
19			Write simple linear and looping scripts		X

Content Experts specify Course that covers Topic and Outcomes with “X”

Map - Citations

	A	B	C	D	E
1			Courses	MAT 135	CIS 210
2	Click here to return to KU Listing				(Click Here) READ THIS FIRST: This matrix is fo
3	**Basic Scripting**				
4		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).			
5		**Topics**			
6			*Basic Security		
7			Bounds checking, input validation		Syl: Wk 3, 6
8			Program Commands		Syl: Wk 1, 6, 8
9			Program Control Structures		Syl: Wk 4, 9, 10
10			Variable Declaration		Syl: Wk 4
11			Debugging		Classroom discussions & demonstrations
12			Scripting Language (e.g. PERL, Python, BASH, VB Scripting, Powershell)		Syl: Wk 3, 4
13			*Basic Boolean logic/operations		
14			AND / OR / XOR / NOT		Wk 3
15		**Outcomes**			
16		Students will be able to:			
17			Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks)		Graded assignments: Manipulate file permissions, work w/ temporary files, create directories, write batch and interactive scripts
18			Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL)		Graded assignments: Parse data, manipulate strings
19			Write simple linear and looping scripts		Graded assignments: Write source code control using RCS

This matrix is for the purpose of mapping curriculum to the NSA/DHS CAE in IA/CD Knowledge Units (KUS). Recommend that you start by filling in individual course numbers that a specific professor or instructor teaches above (ABC-123 is an example), sending the matrix to him or her and having them fill out the KUs by inserting a topic/objective/week/session/etc number that relates to their courses, the initial process is streamlined and less cumbersome. The person charged with the final mappings should then merge the documents into a master and use the master to enter this information in the CAE application website. NOTE: This document may be freely distributed to any institution interested in applying for the NSA/DHS CAE in IA/CD designation. Just delete this text and start filling in the matrix. If you have a better way to do this or a general comment, please email 'askcaeiae@nsa.gov.'

Replace "Xs" with course content using specific references to text, syllabus, course outline, assignments, tests, ...

NSA Recommended Process

- Fill in individual course numbers that a specific professor or instructor teaches
- Send the matrix to him or her to fill out the KUs
- Insert a topic/objective/week/session/etc. number that relates to their courses
- Merge the documents into a master
- Use the master to enter this information in the CAE application website

Course Worksheet

Course Summary Information Mapping Worksheet

Course Number:

Course Title:

Course Creation Date:

Course Last Review Date:

Course Link http://

Course Log-in (User-name & password):

Catalog Description:

Is course currently taught (Y/N)?

Course Length: hours/week & no. of weeks:

Evaluation Methods (select all that apply)
- Chap review,
- Weekly quiz,
- Lab Projects,
- Exams

Instruction Methods (select all that apply)
- Interactive computer,
- Demos,
- Labs,
- Projects,
- Presentations,
- Teamwork,
- Video,
- Remote Learning

Current Enrollment:

Past Enrollment:

Syllabus pdf (upload):

Course Outline pdf (upload):

Is course Active (Y/N)?

Textbook Worksheet

Textbook Form

1. Title of Book or Supplemental Material
2. Relevant Chapter(s)/Title(s)
3. Author

Recap of Important Details

High Level (Overview)

- Text name and author
- Chapter title and number
- Description of material to be covered
- Supplemental material: handouts, notes, workbooks
- Course number & title, creation/review dates, http link, catalog description, course length (no. of hrs), evaluation & instruction methods, past & current enrollment, syllabus/outline, no. of hours

Low Level (Specific - Each Topic)*

- Enter detailed supporting information into Topic/Course cells
- Identify Topic coverage by week, outline references, chapters, assignments, ...
- Outcomes evaluation procedures – tests, presentations, exercises, ...

**Include this info in the cells of the KU matrix!*

Mapping Suggestions

- Involve as many faculty as possible to identify Course Topics and Objectives that satisfy KU Topics and Outcomes.
- Refer to textbook ToC, index and syllabus/detailed course outline to match Course Topics with KU Topics requirements.
- Copy and paste author provided Course Objectives from instructor materials (e.g., presentations) into a text document that can later be used to facilitate entering objectives into the NIETP database.
- Identify how Outcomes will be measured.
- Use the fewest number of courses possible; a single course is more desirable than two.
- One course may be used to map more than one KU.
- Consolidate all “mapping work-product” (i.e., completed spreadsheets, course worksheets, detailed course outlines, syllabus) to expedite data entry.

Phase 2 - Enter Courses (topics & objectives) into database

- Go to NIETP - www.iad.gov/NIETP/
- Login
- Select (or apply for admission to) institution
  - First time: Specify institution information
- Add new or Edit existing course

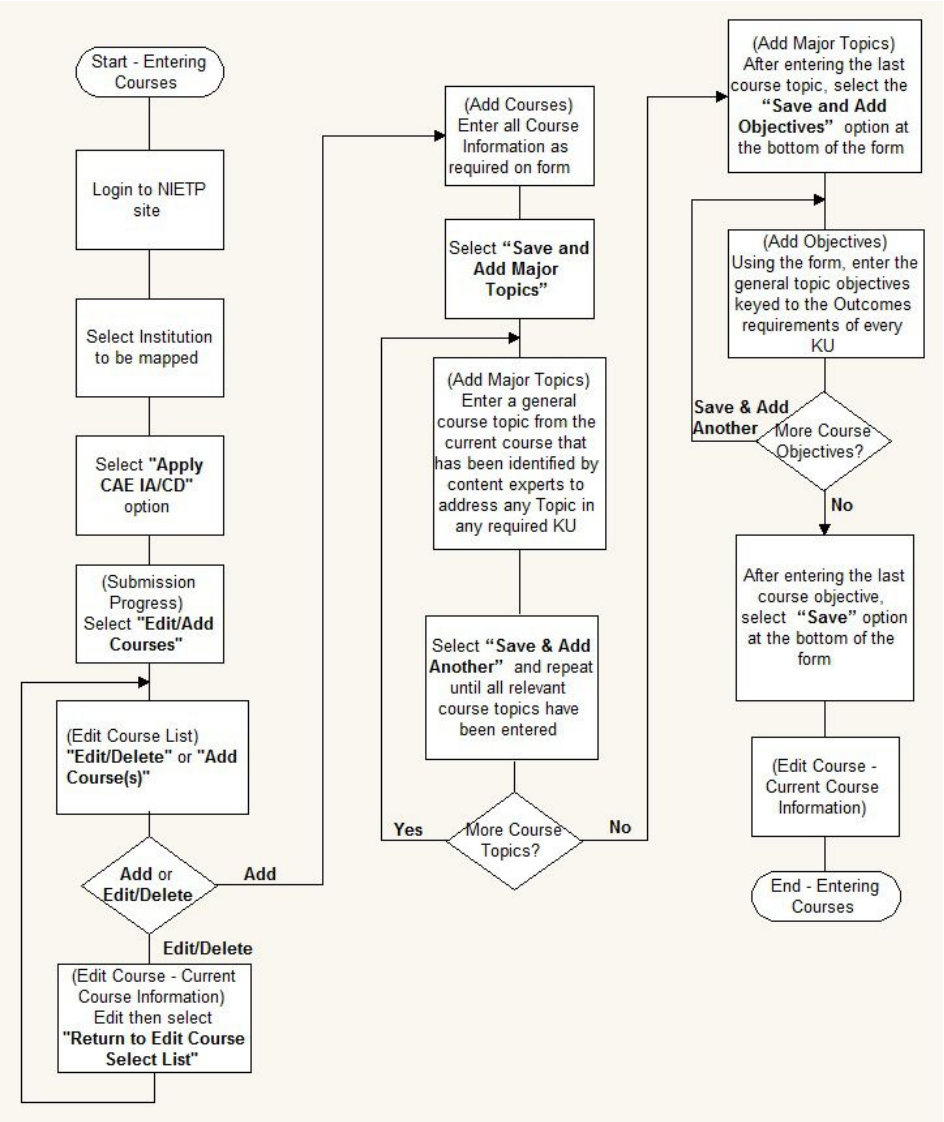
Phase 2: Enter Courses, Topics, & Objectives

Phase 2 (Enter Courses, Topics, Objectives)		
Step	**Operation**	**Note**
1	Login	(**Welcome, Login/Join**)
2	Select Institution to be mapped	(**Institution List**)
3	Select "Apply CAE IA/CD" option	(**Welcome**)
4	In opening screen, select "Add New Courses"	(**CAE Submission xYr Submission**)
5	Enter all Course Information as required on form	(**Add Course**)
6	Select "Save and Add Major Topics"	
7	Using the form, enter a general course topic from the current course that has been identified by content experts to address any Topic in any required KU	(**Add Major Topics for xx**) Course topics come from textbook, syllabus, supplementals, etc.
8	Select "Save & Add Another" and repeat until all relevant course topics have been entered	
9	After entering the last course topic, select the "Save and Add Objectives" option at the bottom of the form	
10	Using the form, enter the general topic objectives keyed to the Outcomes requirements of every KU	(**Add Objectives for xx**) The terminology used in the Objectives should correlate closely with that in the KUs' required Outcomes
11	Select "Save & Add Another" and repeat until all relevant course objectives have been entered	
12	After entering the last course objective, select the "Save" option at the bottom of the form	
13	Once all courses have been identified with topics and objectives relevant to the KUs, the next phase starts.	This concludes identifying the courses, their topics, and objectives

Phase 2 Overview

Enter Courses, Topics & Objectives into Database

"I've got it, too, Omar … a strange feeling like we've just been going in circles."



NIETP Welcome Screen

National IA Education & Training Programs
NIETP

Welcome guest

- Home
- About CAE
- CAE Requirements
- Contact Us
- Security Warnings
- Login / Join

WELCOME

What's New?

NSA/DHS National Centers of Academic Excellence in Information Assurance/Cyber Defense

We are happy to announce that updates to the new NSA/DHS Centers of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD) designation are complete. The creation of this new designation will help distinguish the strengths of each of the CAE institutions, benefitting not only the CAE, but also students, employers and hiring managers throughout the nation.

To review CAE IA/CD Program requirements, please click here.

About The Programs

NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA Education (CAE/IAE), IA 2-year Education (CAE/2Y) and IA Research (CAE/R) programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines. Students attending CAE IA/CD-E and CAE IA/CD-R schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.

CAE IA/CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation's information systems.

NIETP Login (step 1)

National IA Education & Training Programs
NIETP

Welcome guest

- Home
- Contact Us
- Security Warnings
- Login/Join

LOGIN / JOIN

Returning Users Login

Note: **Bold*** items below are required.

Login

All returning users: always login here once your registration is approved.

Login Name *

Password *

Login

New User / Institution	Forgot Password	Forgot Username
To use this site, you must first add your institution and apply for an account using the "New Registration" button.	Forgot your password? We can't reset your password; to reset your password click on the "Forgot Password" button.	Forgot your username? We'll send it to you by email; to receive your username click on the "Forgot Username" button.
New Registration	Forgot Password	Forgot Username

Privacy | Terms of Use | NSA.gov | NoFEAR Act | FOIA | IAD.gov | CNSS.gov

IAD

Select Institution (step 2)

National IA Education & Training Programs
NIETP

Welcome Fred

- Home
- Contact Us
- Security Warnings
- My Institution List
- User Profile
- Logout

IACE Program - Mapping

MY INSTITUTION LIST

Note: **Bold*** items below are required.

Select Institution

Select My Institution

Use this option to modify information (Standards, Criterion, etc.) for Institutions on your Institution List.

My Institution(s) * Sandbox University

Select Institution

Add Institution

Add Another Institution to "My Institutions" List

Use this option to request that another currently listed Institution be added to "My Institutions" list.
Don't see the Institution you want? Use the "Add New Institution" option below.

All Institution(s) * Select Institution...

- Select Institution...
- -- Institution Not listed - Request New Institution --
- Air Force Institute of Technology
- Alabama A&M University
- Albany State University, Georgia
- Alfred State, SUNY College of Technology
- American Public University System
- Anne Arundel Community College
- Arapahoe Community College
- Arizona State University
- Asheville-Buncombe Technical Community College
- Auburn University
- Auburn University at Montgomery
- Augusta State University
- Backbone Security
- Baker College
- Ball State University
- Barton Community College
- Bay de Noc Community College
- Baylor University

Add a New Institution to

Use this option to reque
Not sure if your Institut

Privacy | Te

Logged In Welcome Screen

- Home
- About CAE
- CAE Requirements
- Contact Us
- Security Warnings
- My Institution List
- Edit My Institution(s)
- Submission History
- User Profile
- Logout

CAE Programs

- FA/KU Crosswalk
- CAE Message Center
- Add New Courses
- Edit Existing Courses
- Apply CAE IA/CD
- Apply for CAE-R

IACE Program - Mapping

- IACE Message Center
- Reports & Percentages

WELCOME
SANDBOX UNIVERSITY

What's New?

NSA/DHS National Centers of Academic Excellence in Information Assurance/Cyber Defense

We are happy to announce that updates to the new NSA/DHS Centers of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD) designation are complete. The creation of this new designation will help distinguish the strengths of each of the CAE institutions, benefitting not only the CAE, but also students, employers and hiring managers throughout the nation.

To review CAE IA/CD Program requirements, please click here.

About The Programs

NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA Education (CAE/IAE), IA 2-year Education (CAE/2Y) and IA Research (CAE/R) programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines. Students attending CAE IA/CD-E and CAE IA/CD-R schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.

CAE IA/CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation's information systems.

Application Submissions

NOTE: As of 6/9/2014, forty-three (43) submissions have been received for the CAE IA/CD program.

CAE Application Users

Are you ready to begin your CAE application but do not have an account?

CAE Reference Documents

CAE REQUIREMENTS

All CAE Requirements Criteria documents are PDF files.

- CAE IA/CD 2Yr Criteria
- CAE IA/CD 4Yr Criteria
- CAE IA/CD KU
- CAE IA/CD Focus Areas
- CAE IA/CD Research (CAE-R) Criteria for Redesignation
- CAE IA/CD Research Criteria (CAE-R) for New Institutions

Previous Submissions

- Home
- About CAE
- CAE Requirements
- Contact Us
- Security Warnings
- My Institution List
- Edit My Institution(s)
- Submission History
- User Profile
- Logout

CAE Programs

- FA/KU Crosswalk
- CAE Message Center
- Add New Courses
- Edit Existing Courses
- Apply CAE IA/CD
- Apply for CAE-R

IACE Program - Mapping

- IACE Message Center
- Reports & Percentages

WELCOME
SANDBOX UNIVERSITY

What's New?

NSA/DHS National Centers of Academic Excellence in Information Assurance/Cyber Defense

We are happy to announce that updates to the new NSA/DHS Centers of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD) designation are complete. The creation of this new designation will help distinguish the strengths of each of the CAE institutions, benefitting not only the CAE, but also students, employers and hiring managers throughout the nation.

To review CAE IA/CD Program requirements, please click here.

About The Programs

NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA Education (CAE/IAE), IA 2-year Education (CAE/2Y) and IA Research (CAE/R) programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines. Students attending CAE IA/CD-E and CAE IA/CD-R schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.

CAE IA/CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation's information systems.

Application Submissions

NOTE: As of 6/9/2014, forty-three (43) submissions have been received for the CAE IA/CD program.

CAE Application Users

Are you ready to begin your CAE application but do not have an account?

Previous Submissions

SUBMISSION HISTORY

COLLEGE

Legend

P	The Submission has been Approved.
X	The Submission has been Rejected.
I	The Submission is Incomplete.
R	The Submission has been Recertified.

Overview Submission History

Year	Program	4011	4012	4013E	4013I	4013A	4014E	4014I	4014A	4015	4016E	4016I	4016A
2003	IACE	P											
2006	IACE	P											
2008	IACE			P									
2009	IACE	R											
2010	CAE2Y												
2013	IACE	R		R									

Detailed Submission History

Cycle Year	Program Type	Standard	Status	View
2013	IACE	4011	Recertified	
2013	IACE	4013 - Entry	Recertified	
2010	CAE		Passed	
2009	IACE	4011	Recertified	
2008	IACE	4013 - Entry	Passed	
2006	IACE	4011	Passed	
2003	IACE	4011	Passed	

Add or Edit Course (Step 3)

National IA Education & Training Programs
NIETP

Welcome Fred

- Home
- Contact Us
- Security Warnings
- My Institution List
- Edit My Institution(s)
- Submission History
- User Profile
- Logout

CAE Programs

- About CAE
- CAE Requirements
- CAE Message Center
- Add New Courses
- Edit Existing Courses
- Apply CAE IA/CD

IACE Program - Mapping

- IACE Message Center
- Reports & Percentages

WELCOME

COLLEGE

What's New?

There are no current notices posted.

IA National Centers of Academic Excellence

NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA/CD programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines. Students attending CAE IA/CD-E and CAE IA/CD-R schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.

CAE IA/CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation's information systems.

Privacy | Terms of Use | NSA.gov | NoFEAR Act | FOIA | IAD.gov | CNSS.gov

Add Courses (step 4)

- Home
- Contact Us
- Security Warnings
- My Institution List
- Edit My Institution(s)
- Submission History
- User Profile
- Logout

CAE Programs

- About CAE
- CAE Requirements
- CAE Message Center
- Add New Courses
- Edit Existing Courses
- Apply CAE IA/CD
- Apply for CAE-R

IACE Program - Mapping

- IACE Message Center
- Reports & Percentages

2014 CAE 4YR SUBMISSION PROGRESS
SANDBOX UNIVERSITY

Step 1: Enter Course(s)

Edit/Add Courses — There are currently 1 active courses for Sandbox University

Step 2: Identify KUs and FAs

Identify KU — Edit the Knowledge Units your Institution intends to include in this cycle.

Identify FA — Add the Focus Areas your Institution intends to include in this cycle.

Step 3: Map KUs and FAs using the tables below.

Step 4: Submit Application

Submit CAE IA/CD 4Y — All items in Step 3 must be completed before submitting the application.

Legend

	An (In Progress icon) will appear next to Units that have started.
✔	A ✔ (Completed icon) will appear next to Units that are completed.

Progress	Program Criteria	Action
	CAE IA/CD	Start

Progress	Knowledge Units (KUs)	Action
	Basic Data Analysis	Start
	Basic Scripting	Start
	Cyber Defense	Continue
	Cyber Threats	Start
	Databases	Start
	Fundamental Security Design Principles	Start
	IA Fundamentals	Start
	Intro to Cryptography	Start
	IT System Components	Start
	Network Defense	Start

Add Course (pg1, step 5)

ADD COURSE(S)
SANDBOX UNIVERSITY

Note: **Bold*** items below are required.

Course Information

This field cannot be modified once the record is submitted.

Course Designator/ Course Number *

As represented in your course catalog.

Title *

Enter the date this course was created.

Course Create Date *

Enter the date this course was last reviewed.

Course Review Date *

For verification and review purposes, provide the specific http link for this course (Course website, Angel, Blackboard, etc. - not the course catalog).

Course Link *

[Must begin with "http://" or "https://"]

If needed, please provide a username and password to access the Course Link above.

Course Login

Please provide description as written in your course catalog.

Description *

Is this course currently being taught? * Yes No

Provide the total duration of time in course, hours and weeks (i.e., 30 hours for 30 weeks, 2 one-hour meetings per week).

Course Length *

Add Course (pg2, steps 5 & 6)

Select the evaluation methods utilized in this course. Emphasis should be placed on the evaluation methods used to determine the mastery of the skills/knowledge's associated with the Knowledge Unit(s) the course is being applied against.

Evaluation Methods *

To select/deselect multiple items, hold the CTRL key while clicking.

- Select at least one -
Chapter Reviews
Weekly Quizzes
Lab Projects
Exams

Instruction Methods *

To select/deselect multiple items, hold the CTRL key while clicking.

Projects
Presentations
Teamwork
Video
Remote Learning

Approximately how many students take this course? If it is a new course, please provide projections. Provide the total participation if the course is delivered at multiple locations.

Current Enrollment *

Past Enrollment *

Course Syllabi and Outline Information

Only PDF files may be uploaded. Please virus scan any attachment prior to uploading.

Course Syllabi * Choose File No file chosen

Are the Outline and Syllabi the same? * Yes No

Course Outline * Choose File No file chosen

Save & Exit | Save & Add Major Topics | Cancel

Add Course Topics (steps 7, 8 & 9)

ADD MAJOR TOPICS FOR COMSEC 215 - NETWORK SECURITY FUNDAMENTALS
SANDBOX UNIVERSITY

Note: **Bold*** items below are required.

Major Topics

"Topic" 1 would equate to your week 1, topic 1, chapter 1, session 1, and/or module 1, etc.

Topic Number *

Enter each Major Topic covered in the course emphasizing the topics that address the Knowledge Unit(s) the course is being applied against.

Major Topic *

Add a list of sub-topics covered under this topic. If none, provide a short description of what this Major Topic covers. For non-IA courses, emphasize the topics that address the Knowledge Unit(s).

Topic Description

Is this Topic covered in a Textbook? * Yes No

Is this Topic covered in Supplemental Material? * Yes No

If this Major Topic is covered in either a Textbook or Supplemental Material, provide the Book or Supplemental Material Title.

Book/Supplemental Material

If this Major Topic is covered in either a Textbook or Supplemental Material, provide the Chapter or Title of the article as it appears in the Book or Supplemental Material.

Chapter/Title

If this Major Topic is covered in either a Textbook or Supplemental Material, provide the Author of the Book or Supplemental Material.

Author

Save & Add Another | Save & Add Objectives | Save | Cancel

Add Course Objectives (step 10, 11, & 12)

ADD OBJECTIVES FOR COMSEC 215 - NETWORK SECURITY FUNDAMENTALS
SANDBOX UNIVERSITY

Note: **Bold*** items below are required.

Objectives

Objective Number *

Broadly list the competencies achieved in this course or what the learner must be able to perform in order to demonstrate the mastery of the objectives.

Objective

Save & Add Another | Save | Cancel

Added Course Example (p. 1 of 2)

ADD COURSE(S)
SANDBOX UNIVERSITY

Note: **Bold*** items below are required.

Course Information

This field cannot be modified once the record is submitted.

Course Designator/ Course Number *: COSC 3365

As represented in your course catalog.

Title *: Cyber Defense I

Enter the date this course was created.

Course Create Date *: 01/15/2013

Enter the date this course was last reviewed.

Course Review Date *: 01/15/2014

For verification and review purposes, provide the specific http link for this course (Course website, Angel, Blackboard, etc. - not the course catalog).

Course Link *: faculty.tamucc.edu/.../SyllabusSpr2013/Syllabus-CyberDef%2(

[Must begin with "http://" or "https://"]

If needed, please provide a username and password to access the Course Link above.

Course Login:

Please provide description as written in your course catalog.

Description *: This course introduces the student to the identification of vulnerabilities, forms of attack, appropriate countermeasures, and the detection and defense of the same. Tools and techniques for the securing of hardware, software and data, including physical security

Is this course currently being taught? *: Yes No

Added Course Example (p. 2 of 2)

Is this course currently being taught? * Yes No

Provide the total duration of time in course, hours and weeks (i.e., 30 hours for 30 weeks, 2 one-hour meetings per week).

Course Length * 45 hours for 15 weeks; 2 one-and-a-half hour meetings per we

Select the evaluation methods utilized in this course. Emphasis should be placed on the evaluation methods used to determine the mastery of the skills/knowledge's associated with the Knowledge Unit(s) the course is being applied against.

Evaluation Methods * To select/deselect multiple items, hold the CTRL key while clicking.

- Select at least one -
Chapter Reviews
Weekly Quizzes
Lab Projects
Exams

Instruction Methods * To select/deselect multiple items, hold the CTRL key while clicking.

Projects
Presentations
Teamwork
Video
Remote Learning

Approximately how many students take this course? If it is a new course, please provide projections. Provide the total participation if the course is delivered at multiple locations.

Current Enrollment * 35

Past Enrollment * 35

Course Syllabi and Outline Information

Only PDF files may be uploaded. Please virus scan any attachment prior to uploading.

Course Syllabi * Choose File Sandbox Uni...SC 3365.doc

Are the Outline and Syllabi the same? * Yes No

Course Outline * Choose File No file chosen

Save & Exit | Save & Add Major Topics | Cancel

Added Course Topic Example

ADD MAJOR TOPICS FOR COSC 3365 - CYBER DEFENSE I
SANDBOX UNIVERSITY

Note: **Bold*** items below are required.

Major Topics

"Topic" 1 would equate to your week 1, topic 1, chapter 1, session 1, and/or module 1, etc.

Topic Number *: 1

Enter each Major Topic covered in the course emphasizing the topics that address the Knowledge Unit(s) the course is being applied against.

Major Topic *: pping (enumeration and identification of network components)

Add a list of sub-topics covered under this topic. If none, provide a short description of what this Major Topic covers. For non-IA courses, emphasize the topics that address the Knowledge Unit(s).

Topic Description:
Monitoring critical areas, communications centers, info sys centers, protected distribute systems, stand-alones, peripherals, storage areas.
Explain access controls & monitoring to, access to doors & entry points, layered access controls, physical security perimeters

Is this Topic covered in a Textbook? * (•) Yes ( ) No

Is this Topic covered in Supplemental Material? * ( ) Yes (•) No

If this Major Topic is covered in either a Textbook or Supplemental Material, provide the Book or Supplemental Material Title.

Book/Supplemental Material: All in One CompTIA Security +

If this Major Topic is covered in either a Textbook or Supplemental Material, provide the Chapter or Title of the article as it appears in the Book or Supplemental Material.

Chapter/Title: Physical Security - Chapter 7 Physical Security; Chapter 12 Se

If this Major Topic is covered in either a Textbook or Supplemental Material, provide the Author of the Book or Supplemental Material.

Author:

Save & Add Another | Save & Add Objectives | Save | Cancel

Added Course Objective Example

ADD OBJECTIVES FOR COSC 3365 - CYBER DEFENSE I
SANDBOX UNIVERSITY

Note: **Bold*** items below are required.

Objectives

Objective Number * 1

Broadly list the competencies achieved in this course or what the learner must be able to perform in order to demonstrate the mastery of the objectives

Objective: Student will identify various potential system attack methods including social engineering, denial of service, Trojans, logic bombs, database inference, man-in-the-middle, etc. Graded written exams will assess their understanding of ability to recognize attack methods.

Save & Add Another | Save | Cancel

Course, Topic, Objective
In Progress - 1 Topic, 1 Objective

Course Number	COSC 3365
Title	Cyber Defense I
Course Created	01/15/2013
Course Last Reviewed	01/15/2014
Course Link	http://sandboxU.edu
Course Login	
Description	This course introduces the student to the identification of vulnerabilities, forms of attack, appropriate countermeasures, and the detection and defense of the same. Tools and techniques for the securing of hardware, software and data, including physical security are covered. The issues and facilities available to both the intruder and administrator will be examined and evaluated with appropriate exercises to illustrate their effect.
Is Currently Taught	Yes
Course Length	45 hours for 15 weeks; 2 one-and-a-half hour meetings per week
Current Enrollment	35
Past Enrollment	35
Instruction Methods	Lecture,Demonstrations,Labs,Projects
Evaluation Methods	Lab Projects,Exams
Syallabus	Sandbox Univ Syllabus-CyberDef I COSC 3365.pdf
Outline	Sandbox Univ Syllabus-CyberDef I COSC 3365.pdf
Is Active	Yes

Add a Major Topic for Course COSC 3365

	Major Topics for COSC 3365	Active	Edit/Delete
1	Potential Attack Methods	✓	

Add an Objective for Course COSC 3365

	Objectives for COSC 3365	Active	Edit/Delete
1	Student will identify various potential system attack methods including social engineering, denial of service, Trojans, logic bombs, database inference, man-in-the-middle, etc. Graded written exams will assess their understanding of ability to recognize attack methods.	✓	

Return to Edit Course Select List.

Completed Course Summary

Course Information for COMSEC 215

Edit/Delete Course Information for COMSEC 215

View Complete Course Information

Course Number	COMSEC 215
Title	Network Security Fundamentals
Course Created	07/19/2013
Course Last Reviewed	01/19/2014
Course Link	http://sandbox.edu/Course/COMSEC215
Course Login	
Description	Provides an introduction to the fundamentals of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The course covers new topics in network security as well, including psychological approaches to social engineering attacks, Web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security. Students will also engage in activities that link to the Information Security Community Site.
Is Currently Taught	Yes
Course Length	45 hours for 15 weeks, 2 one-and-a-half meetings per week
Current Enrollment	95
Past Enrollment	95
Instruction Methods	Lecture,Demonstrations,Labs,Projects,Teamwork
Evaluation Methods	Chapter Reviews,Lab Projects,Exams
Syallabus	Syllabus COMSEC 215.pdf
Outline	Syllabus COMSEC 215.pdf
Is Active	Yes

Add a Major Topic for Course COMSEC 215

	Major Topics for COMSEC 216	Active	Edit/Delete
Week 1	Intro to Security	✓	
Week 10	Authentication and Account Management	✓	
Week 11	Basic Cryptography	✓	
Week 12	Advanced Cryptography	✓	
Week 13	Business Continuity	✓	
Week 14	Risk Management	✓	
Week 2	Malware and Social Engineering Attacks	✓	
Week 3	Application and Network Attacks	✓	
Week 4	Vulnerability Assessment and Mitigating Attacks	✓	
Week 5	Host, Application, and Data Security	✓	
Week 6	Network Security	✓	
Week 7	Administering a Secure Network	✓	
Week 8	Wireless Network Security	✓	
Week 9	Access Control Fundamentals	✓	

Add an Objective for Course COMSEC 215

	Objectives for COMSEC 216	Active	Edit/Delete
1	Define information security; Explain importance of information security; Describe challenges of securing information; Identify types of attackers; List basic steps of an attack; Describe the five basic principles of defense.	✓	
2	Describe difference between virus and worm; List types of malware that conceals its existence; Identify kinds of malware designed for profit; Describe types of social engineering attacks; Explain physical social engineering attacks.	✓	
3	List and explain different types of Web application attacks; Define client-side attacks; Explain buffer overflow attack process; List types of DoS (denial of service) attacks; Describe interception and poisoning attacks.	✓	
4	Define vulnerability assessment, explain why it's important; List vulnerability assessment techniques and tools; Explain differences between vulnerability scanning and penetration tools; List techniques to mitigate and deter attacks.	✓	
5	List steps to secure a host computer; Define application security; Explain how to secure data using data loss prevention.	✓	
6	List different types of network security devices; Explain how network security devices can be used; Define NAT (network address translation; Define NAC (network access control); Explain how to enhance security through network design.	✓	
7	List and describe functions of common network protocols; Explain how network administration principles can be applied; Define new types of network applications; Explain how network applications can be secured.	✓	
8	Describe different types of wireless network attacks; List vulnerabilities of IEEE 802.11 security; Explain solutions for securing wireless network.	✓	
9	Define access control; List the four access control methods; Explain the different types of physical access control; Define authentication services.	✓	
10	Describe the three types of authentication credentials; Explain what single sign-on can do; List account management procedures for securing passwords; Define trusted operating systems.	✓	
11	Define cryptography and elements of a cryptographic system; Describe hash, symmetric, and asymmetric cryptographic algorithms; List various ways in which cryptography is used.	✓	
12	Define digital certificates; List various types of digital certificates and how they are used; Describe components of PKI (Public Key Infrastructure); Explain strengths and weaknesses of cryptographic systems; List tasks associate with key management; Different the different transport encryption algorithms.	✓	
13	Define environmental controls; Describe components of redundancy planning; List disaster recovery procedures; Describe incident response procedures.	✓	
14	Explain how to control risk; List the types of security policies; Describe how awareness and training can provide increased security.	✓	

Phase 3 - Match Courses to Intended KUs

- Go to NIETP - www.iad.gov/NIETP/
- Login
- Select institution
- Select “Apply CAE IA/CD”
- Intent List - "Identify KUs"

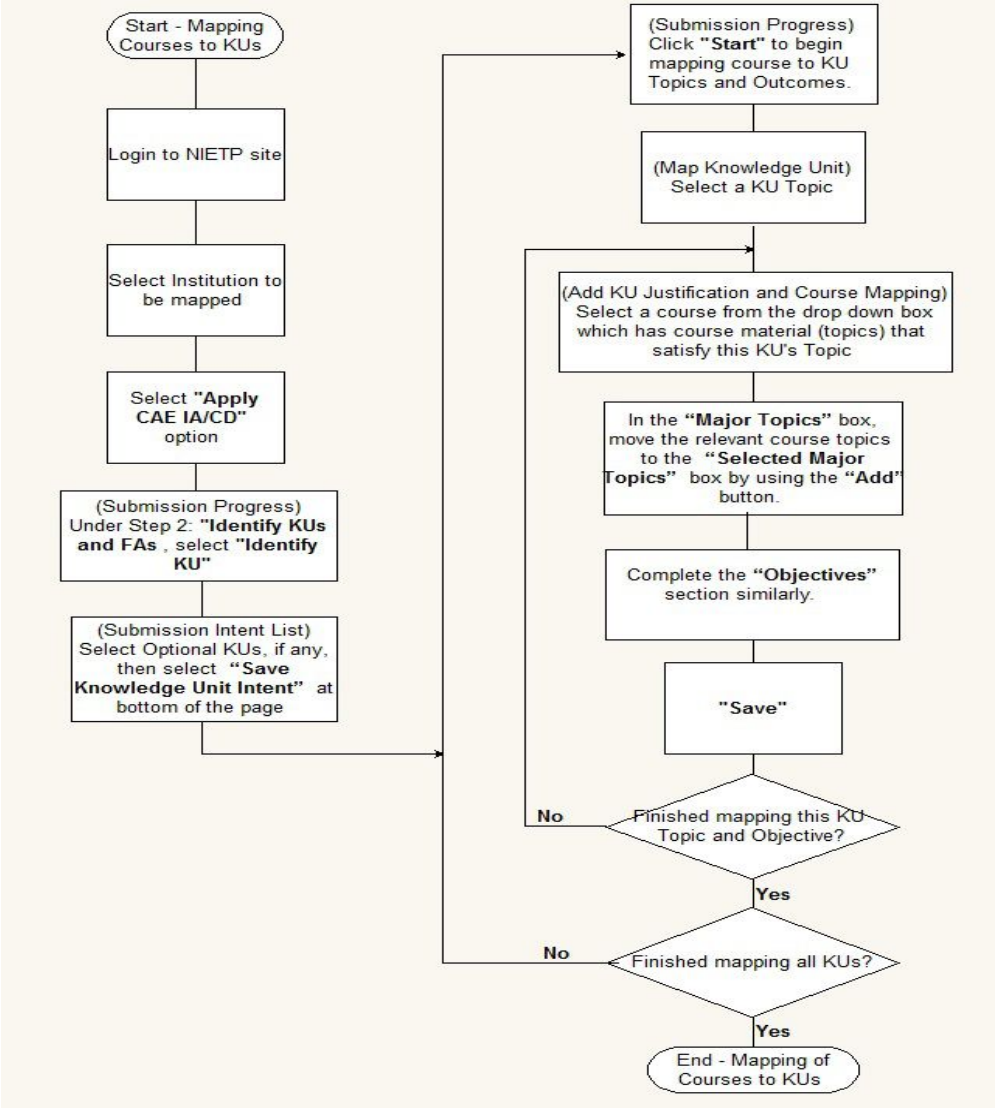
Why they're called bullet points.

Phase 3: Step-by-Step Table

Phase 3 : Map Courses to KUs		
Step	**Operation**	**Note**
14	Repeat steps 1, 2, and 3 of Phase 2	
15	Under “Step 2: Identify KUs and FAs” of the opening form, select “Identify KU” box	**(Submission Progress)**
16	The next screen selects all mandatory KUs for the level of your institution. If institution is 4 yr, 5 additional KUs must be selected. Select “Save Knowledge Unit Intent” at bottom of the page	**(Submission Intent List)** At the conclusion of this step, all KUs that are intended to be mapped by this institution should have been identified
17	This screen returns to the Submission Progress screen lists all KUs that the institution plans to map. “Start” identifies a KU, none of whose Topics or Outcomes has yet been addressed. “Continue” identifies a KU whose mapping has been initiated.	**(Submission Progress)**
18	Click “Start” (or “Continue”) on a KU to be mapped	
19	A screen appears with a list Topics and Outcomes defining that KU. Select a Topic or Outcome to map.	**(Map Knowledge Unit)**
20	On the next screen, select a course from the drop down box which has course material (topics) that satisfy this KU's Topic	**(Add KU Justification and Course Mapping)**
21*	In the “Major Topics” box, move the relevant course topics to the “Selected Major Topics” box by using the “Add” button.	
22*	Repeat the process for the “Objectives” section.	
*	*Alternative to steps 21 & 22, enter “Justification”	Use Justification when KU is satisfied by pre-req or means other than coursework.
23	“Save”	
24	Repeat the process from step 18 until every KU Topic and Outcome has been mapped by current course.	**(Map Knowledge Unit)**
25	Repeat the process from step 17 until all KUs have been mapped for all courses.	

Phase 3 Overview

Match courses to KU requirements



Identify KUs to be Mapped (step 15)

2014 CAE 4YR SUBMISSION PROGRESS
SANDBOX UNIVERSITY

Step 1: Enter Course(s)

Edit/Add Courses — There are currently 3 active courses for Sandbox University

Step 2: Identify KUs and FAs

Identify KU — Edit the Knowledge Units your Institution intends to include in this cycle.

Identify FA — Add the Focus Areas your Institution intends to include in this cycle.

Step 3: Map KUs and FAs using the tables below.

Step 4: Submit Application

Submit CAE IA/CD 4Y — All items in Step 3 must be completed before submitting the application.

Legend

	An (In Progress icon) will appear next to Units that have started.
✔	A ✔ (Completed icon) will appear next to Units that are completed.

Progress	Program Criteria	Action
	CAE IA/CD	Start

Progress	Knowledge Units (KUs)	Action
	Basic Data Analysis (Core)	Start
	Basic Scripting (Core)	Start
	Cyber Defense (Core)	Continue
	Cyber Threats (Core)	Continue
	Databases (Core)	Start
	Fundamental Security Design Principles (Core)	Start
	IA Fundamentals (Core)	Continue
✔	Intro to Cryptography (Core)	Edit
	IT System Components (Core)	Start

- By default, next screen selects all mandatory KUs for the level of the institution.
  - If 4 yr institution, 5 additional KUs must be selected
  - Optional, if any, KUs must be identified in order to proceed
- Select “Save Knowledge Unit Intent” (bottom of screen)

2 Yr KU Submission Intent List (step 16)

2014 CAE2Y KU SUBMISSION INTENT LIST
ANNE ARUNDEL COMMUNITY COLLEGE

1. Select the Knowledge Units (KUs) your Institution intends to submit.
2. Knowledge Units that have already been successfully accredited will be noted below.
3. All Knowledge Units listed in the Core section are required.
4. At a minimum, the required number of Optional Knowledge Units must be selected.
5. Click on any Knowledge Unit title to see its associated Focus Areas (FAs).

Core Knowledge Units (All are Required)

Knowledge Unit	Intend to Map?
Basic Data Analysis	Yes (Required)
Basic Scripting	Yes (Required)
Cyber Defense	Yes (Required)
Cyber Threats	Yes (Required)
Fundamental Security Design Principles	Yes (Required)
IA Fundamentals	Yes (Required)
Intro to Cryptography	Yes (Required)
IT System Components	Yes (Required)
Networking Concepts	Yes (Required)
Policy, Legal, Ethics and Compliance	Yes (Required)
Systems Administration	Yes (Required)

Optional Knowledge Units (0 Required)

Knowledge Unit	Intend to Map?
Advanced Cryptography	Yes No
Advanced Network Technology and Protocols	Yes No
Algorithms	Yes No
Analog Telecommunications Systems	Yes No
Cloud Computing	Yes No
Cybersecurity Planning and Management	Yes No
Data Administration	Yes No
Data Structures	Yes No
Database Management Systems	Yes No
Databases	Yes No

4 Yr KU Submission Intent List (step 16)

2014 CAE4Y KU SUBMISSION INTENT LIST
SANDBOX UNIVERSITY

1. Select the Knowledge Units (KUs) your Institution intends to submit.
2. Knowledge Units that have already been successfully accredited will be noted below.
3. All Knowledge Units listed in the Core section are required.
4. At a minimum, the required number of Optional Knowledge Units must be selected.
5. Click on any Knowledge Unit title to see its associated Focus Areas (FAs).

Core Knowledge Units (All are Required)

Knowledge Unit	Intend to Map?
Basic Data Analysis	Yes (Required)
Basic Scripting	Yes (Required)
Cyber Defense	Yes (Required)
Cyber Threats	Yes (Required)
Databases	Yes (Required)
Fundamental Security Design Principles	Yes (Required)
IA Fundamentals	Yes (Required)
Intro to Cryptography	Yes (Required)
IT System Components	Yes (Required)
Network Defense	Yes (Required)
Network Technology and Protocols	Yes (Required)
Networking Concepts	Yes (Required)
Operating Systems Concepts	Yes (Required)
Policy, Legal, Ethics and Compliance	Yes (Required)
Probability and Statistics	Yes (Required)
Programming	Yes (Required)
Systems Administration	Yes (Required)

Optional Knowledge Units (5 Required)

Knowledge Unit	Intend to Map?
Advanced Cryptography	Yes No
Advanced Network Technology and Protocols	Yes No
Algorithms	Yes No
Analog Telecommunications Systems	Yes No
Cloud Computing	Yes No
Cybersecurity Planning and Management	Yes No
Data Administration	Yes No
Data Structures	Yes No

KU Submission Intent List (step 16)

+ IA Compliance	Yes No
+ IA Standards	Yes No
Independent Study / Directed Study / Special Topics / Advanced Topics	Yes No
+ Industrial Control Systems	Yes No
Intro to Theory of Computation	Yes No
+ Intrusion Detection / Prevention Systems	Yes No
+ Life-Cycle Security	Yes No
+ Low Level Programming	Yes No
+ Media Forensics	Yes No
+ Mobile Technologies	Yes No
+ Network Forensics	Yes No
+ Network Security Administration	Yes No
+ Operating Systems Hardening	Yes No
+ Operating Systems Theory	Yes No
+ Overview of Cyber Operations	Yes No
+ Penetration Testing	Yes No
+ Policy, Legal, Ethics and Compliance	Yes No
+ QA / Functional Testing	Yes No
+ RF Principles	Yes No
+ Secure Programming Practices	Yes No
+ Security Program Management	Yes No
+ Security Risk Analysis	Yes No
+ Software Assurance	Yes No
+ Software Reverse Engineering	Yes No
+ Software Security Analysis	Yes No
+ Supply Chain Security	Yes No
+ Systems Certification and Accreditation	Yes No
+ Systems Programming	Yes No
+ Systems Security Engineering	Yes No
+ Virtualization Technologies	Yes No
+ Vulnerability Analysis	Yes No
+ Wireless Sensor Networks	Yes No

NOTE

Removing a Knowledge Unit "Intend to Map" will remove all Focus Area "Intend to Map" where the Knowledge Unit is required.

Save Knowledge Unit Intent | Cancel Changes

Select KU That Course Topics and Objectives Will Map To (steps 17 & 18)

2014 CAE 4YR SUBMISSION PROGRESS
SANDBOX UNIVERSITY

Step 1: Enter Course(s)
Edit/Add Courses — There are currently 1 active courses for Sandbox University

Step 2: Identify KUs and FAs
Identify KU — Edit the Knowledge Units your Institution intends to include in this cycle.
Identify FA — Add the Focus Areas your Institution intends to include in this cycle.

Step 3: Map KUs and FAs using the tables below.

Step 4: Submit Application
Submit CAE IA/CD 4Y — All items in Step 3 must be completed before submitting the application.

Legend

	An (In Progress icon) will appear next to Units that have started.
✔	A ✔ (Completed icon) will appear next to Units that are completed.

Progress	Program Criteria	Action
	CAE IA/CD	Start

Progress	Knowledge Units (KUs)	Action
	Basic Data Analysis	Start
	Basic Scripting	Start
	Cyber Defense	Continue
	Cyber Threats	Start
	Databases	Start
	Fundamental Security Design Principles	Start
	IA Fundamentals	Start
	Intro to Cryptography	Start
	IT System Components	Start

Select KU Topic to Map (step 19)

MAP KNOWLEDGE UNIT: IT SYSTEM COMPONENTS
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List.

Legend

	You will see the top-level icon (up arrow) next to Top-Level Items that do NOT need to be mapped.
	You will see the lower-level icon (bent-pipe) next to Lower-Level Items that need to be mapped.
✓	You will see the ✓ completed icon (checkmark) next to Items that have been mapped.

Knowledge Unit Topics & Outcomes

Mapped	Topic
	Guards / CDSes / VPNs / Firewalls
	IDSes, IPSes
	Mobile Devices
	Network Storage Devices
	Peripheral Devices / Security Peripherals
	Routers / Switches / Gateways
	Servers
	Workstations

Mapped	Outcome
	Students will be able to describe the hardware components of modern computing environments and their individual functions.

Return to CAE IA/CD Progress List.

Select Course(s) & Course Topic(s) to Map to KU Topic (step 20 & 21)

ADD KU JUSTIFICATION AND COURSE MAPPING
SANDBOX UNIVERSITY

Selected KU Topic

IT 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.

→ Network Storage Devices

General Instructions

- You must specify whether you will be mapping to a course.
- If you select 'Yes' to mapping a Course, you MUST select at least one Major Topic OR Objective .
- If you select 'No' to mapping a Course, you MUST enter a Justification .
- If you "Select Another Course" you can continue to enter information, but the information entered on this screen is not saved until you select the "Save" button.
- Selecting "Cancel" at any point in this process will delete all the information entered since your last "Save."

Note: **Bold*** items below are required.

Step 1: Map a course?

Will you be mapping one or more courses to this KU Topic? (If using a prerequisite course not entered in this application, select 'No' and enter that information in the Justification.)

Map a course? * ● Yes ○ No If 'No' is selected, you MUST provide a justification.

Step 2: SelectCourse

Select a Course to satisfy this KU Topic. If other Courses have already been selected, you can add another Course.

Course COMSEC 215 - Network Security Fundamentals

Step 3: Select Major Topics

Select one or more Major Topic used to satisfy this KU Topic. Click the "Add" button to move them to the Selected Major Topics box. You can remove a Major Topic from the Selected Major Topics box by selecting the item and clicking the "Remove" button.

Major Topics

Week 1: Intro to Security
Week 10: Authentication and Account Management
Week 11: Basic Cryptography
Week 12: Advanced Cryptography

Add Remove

Selected Major Topics *

Select Course(s) & Objective(s) to Map to KU Topic (step 20 & 21)

Step 4: Select Objectives

*Select **one or more** Objectives used to satisfy this KU Topic. Click the "Add" button to move them to the Selected Objectives box. You can remove a Objectives from the Selected Objectives box by selecting the item and clicking the "Remove" button.*

Objectives

1: Define information security; Explain importance of inforr
2: Describe difference between virus and worm; List type
3: List and explain different types of Web application attac
4: Define vulnerability assessment, explain why it's import

Add Remove

Selected Objectives *

Step 5: Justification

Justification is optional if you are mapping to a topic.
Justification is required if you are NOT mapping to a topic.

If you are NOT mapping to a topic, please identify how the knowledge and/or skill of this KU topic has been obtained. Examples may include pre-requisite knowledge gained from previous courses at a prior institution, alternative coursework, exposure to labs, internship opportunities or any information that establishes an equivalency that adequately prepares the student to meet the outcomes of this Knowledge Unit.

Justification * N/A

Reminders!

- You must specify whether you will be mapping to a course.
- If you select 'Yes' to mapping a Course, you MUST select at least one Major Topic OR Objective.
- If you select 'No' to mapping a Course, you MUST enter a Justification.
- If you "Select Another Course" you can continue to enter information, but the information entered on this screen is not saved until you select the "Save" button.
- Selecting "Cancel" at any point in this process will delete all the information entered since your last "Save."

Save | Select Another Course | Cancel

Select KU's Outcome(s) to Map (step 22)

MAP KNOWLEDGE UNIT: IT SYSTEM COMPONENTS
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List.

Legend

	You will see the top-level icon (up arrow) next to Top-Level Items that do NOT need to be mapped.
	You will see the lower-level icon (bent-pipe) next to Lower-Level Items that need to be mapped.
✓	You will see the ✓ completed icon (checkmark) next to Items that have been mapped.

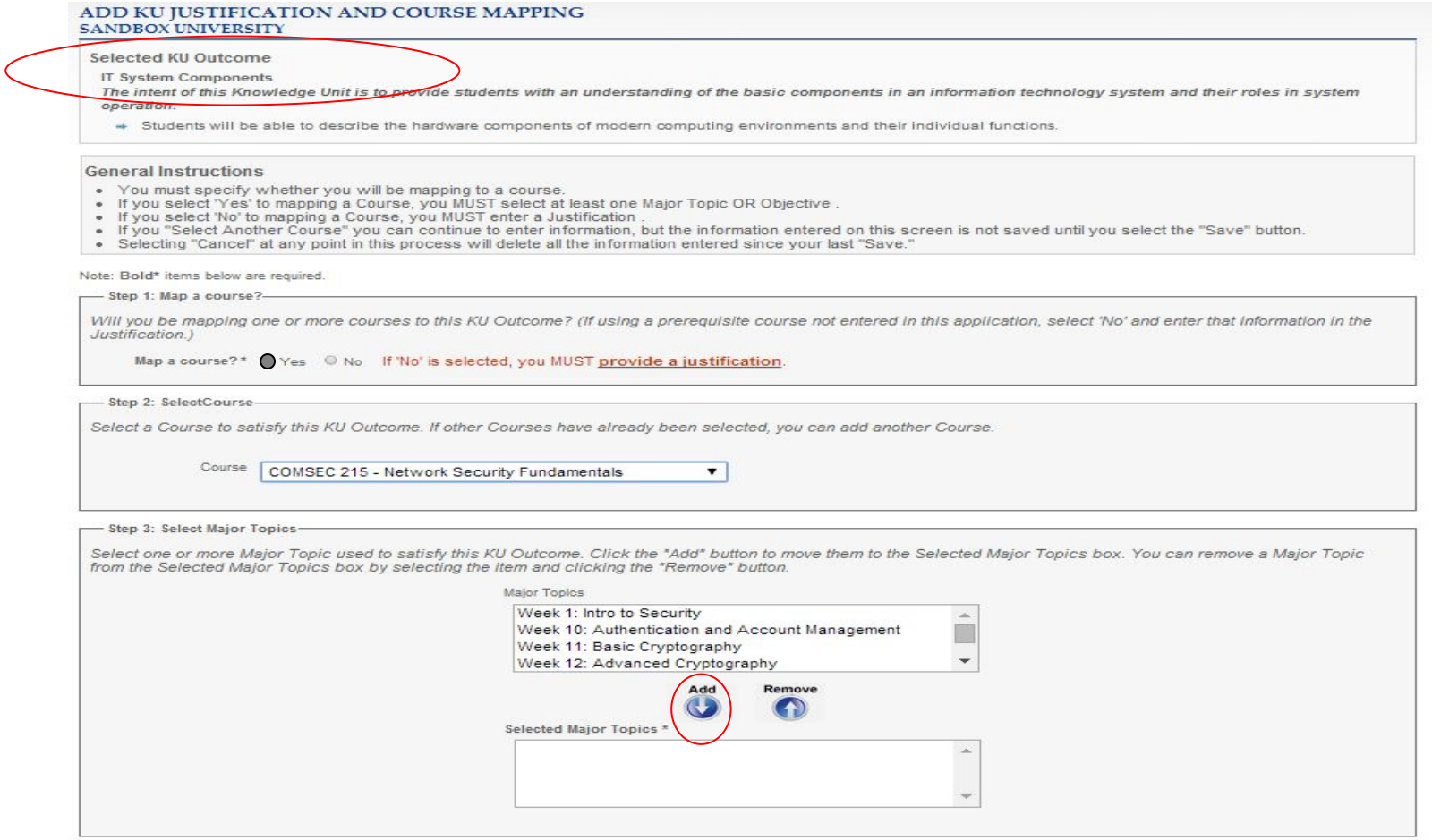
Knowledge Unit Topics & Outcomes

Mapped	Topic
	Guards / CDSes / VPNs / Firewalls
	IDSes, IPSes
	Mobile Devices
	Network Storage Devices
	Peripheral Devices / Security Peripherals
	Routers / Switches / Gateways
	Servers
	Workstations

Mapped	Outcome
	Students will be able to describe the hardware components of modern computing environments and their individual functions.

Return to CAE IA/CD Progress List.

Select Course and Course Topic(s) to Satisfy KU Outcome



Select Course Objectives and Specify Justification to Meet KU Outcome

Step 4: Select Objectives

*Select **one or more** Objectives used to satisfy this KU Outcome. Click the "Add" button to move them to the Selected Objectives box. You can remove a Objectives from the Selected Objectives box by selecting the item and clicking the "Remove" button.*

Objectives

11: Define cryptography and elements of a cryptographic
12: Define digital certificates; List various types of digital c
13: Define environmental controls; Describe components c
14: Explain how to control risk; List the types of security p

Add Remove

Selected Objectives *

Step 5: Justification **Only if Course is not mapped to KU**

Justification is required..
Please indicate how you determine this outcome is met. Examples may include any projects, exercises and/or labs that support this outcome. Outcomes may also be met by pre-requisite knowledge gained from previous courses at a prior institution, alternative coursework, exposure to labs, internship opportunities or any information that establishes an equivalency that adequately prepares the student to meet the outcomes of this Knowledge Unit.

Justification *

Reminders!

- You must specify whether you will be mapping to a course.
- If you select 'Yes' to mapping a Course, you MUST select at least one Major Topic OR Objective.
- If you select 'No' to mapping a Course, you MUST enter a Justification.
- If you "Select Another Course" you can continue to enter information, but the information entered on this screen is not saved until you select the "Save" button.
- Selecting "Cancel" at any point in this process will delete all the information entered since your last "Save."

Save | Select Another Course | Cancel

Completed Mapping Sample

2014 CAE 4YR SUBMISSION PROGRESS
SANDBOX UNIVERSITY

Step 1: Enter Course(s)

Edit/Add Courses — There are currently 3 active courses for Sandbox University

Step 2: Identify KUs and FAs

Identify KU — Edit the Knowledge Units your Institution intends to include in this cycle.

Identify FA — Add the Focus Areas your Institution intends to include in this cycle.

Step 3: Map KUs and FAs using the tables below.

Step 4: Submit Application

Submit CAE IA/CD 4Y — All items in Step 3 must be completed before submitting the application.

Legend

	An (In Progress icon) will appear next to Units that have started.
✔	A ✔ (Completed icon) will appear next to Units that are completed.

Progress	Program Criteria	Action
	CAE IA/CD	Start

Progress	Knowledge Units (KUs)	Action
	Basic Data Analysis (Core)	Start
	Basic Scripting (Core)	Start
	Cyber Defense (Core)	Continue
	Cyber Threats (Core)	Continue
	Databases (Core)	Start
	Fundamental Security Design Principles (Core)	Start
	IA Fundamentals (Core)	Continue
✔	Intro to Cryptography (Core)	Edit
	IT System Components (Core)	Start
	Network Defense (Core)	Start
	Network Technology and Protocols (Core)	Start
	Networking Concepts (Core)	Start

Completed KU Mapping Sample
Topic Drill Down

MAP KNOWLEDGE UNIT: INTRO TO CRYPTOGRAPHY
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List.

Legend

	You will see the top-level icon (up arrow) next to Top-Level Items that do NOT need to be mapped.
	You will see the lower-level icon (bent-pipe) next to Lower-Level Items that need to be mapped.
✓	You will see the ✓ completed icon (checkmark) next to Items that have been mapped.

Knowledge Unit Topics & Outcomes

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

Mapped	Outcome
✓	Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.
✓	Students will be able to describe the differences between symmetric and asymmetric algorithms.
✓	Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
✓	Students will be able to identify the elements of a cryptographic system.

Return to CAE IA/CD Progress List.

Mapped Sample - Topic/Objective Detail

MAPPED KU ITEM
SANDBOX UNIVERSITY

Return to Map KU List

Selected KU Topic

Intro to Cryptography
The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.
→ Digital Signatures (Authentication)

Legend

	If a course is mapped in a Submitted Standard that is still being reviewed, only limited course information may be edited. You will see a (view icon) next to the items that are locked.
	Once the Submitted Standard Review is completed the course information will be released for edit. You will see the (edit icon) next to the items that are available for edit.
	You will see an (add icon) next to the items when you can add another Course selection.

Justification for Selected KU Item

Edit Justification

Delete Justification and ALL Course Mappings

Justification
N/A

Course(s) Mapped to Selected KU Topic

Add Another Course Selection

COMSEC 215 - Network Security Fundamentals
Edit COMSEC 215 Course Selection

Delete COMSEC 215 Mapping

Major Topics for COMSEC 215	
Week 11	Basic Cryptography
Week 12	Advanced Cryptography

Objectives for COMSEC 215	
11	Define cryptography and elements of a cryptographic system; Describe hash, symmetric, and asymmetric cryptographic algorithms; List various ways in which cryptography is used.
12	Define digital certificates; List various types of digital certificates and how they are used; Describe components of PKI (Public Key Infrastructure); Explain strengths and weaknesses of cryptographic systems; List tasks associate with key management; Different the different transport encryption algorithms.

Return to Map KU List

Completed Mapping Sample
Outcome Drill Down

MAP KNOWLEDGE UNIT: INTRO TO CRYPTOGRAPHY
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List.

Legend

	You will see the top-level icon (up arrow) next to Top-Level Items that do NOT need to be mapped.
	You will see the lower-level icon (bent-pipe) next to Lower-Level Items that need to be mapped.
✓	You will see the ✓ completed icon (checkmark) next to Items that have been mapped.

Knowledge Unit Topics & Outcomes

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

Mapped	Outcome
✓	Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.
✓	Students will be able to describe the differences between symmetric and asymmetric algorithms.
✓	Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
✓	Students will be able to identify the elements of a cryptographic system.

Return to CAE IA/CD Progress List.

Mapped Sample - Outcome Detail

MAPPED KU ITEM
SANDBOX UNIVERSITY

Return to Map KU List

Selected KU Outcome

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

- Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.

Legend

	If a course is mapped in a Submitted Standard that is still being reviewed, only limited course information may be edited. You will see a (view icon) next to the items that are locked.
	Once the Submitted Standard Review is completed the course information will be released for edit. You will see the (edit icon) next to the items that are available for edit.
	You will see an (add icon) next to the items when you can add another Course selection.

Justification for Selected KU Item

Edit Justification

Delete Justification and ALL Course Mappings

Justification
Hands-On Project 5-1: Use a Symmetric Algorithm in Word 2010 to encrypt confidential messages. Hands-On Assignment: Use public key exchange generating private and public keys to exchange encrypted messages with instructor.

Course(s) Mapped to Selected KU Outcome

Add Another Course Selection

COMSEC 215 - Network Security Fundamentals
Edit COMSEC 215 Course Selection

Delete COMSEC 215 Mapping

Major Topics for COMSEC 215	
Week 1	Intro to Security
Week 11	Basic Cryptography
Week 12	Advanced Cryptography

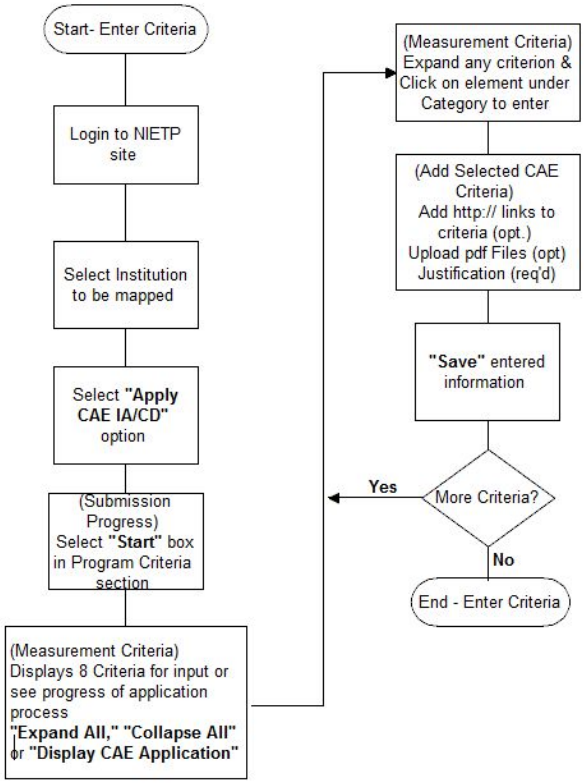
Objectives for COMSEC 215	
12	Define digital certificates; List various types of digital certificates and how they are used; Describe components of PKI (Public Key Infrastructure); Explain strengths and weaknesses of cryptographic systems; List tasks associate with key management; Different the different transport encryption algorithms.

Return to Map KU List

End of Phase 3

Repeat the above… Adding and mapping Courses to KU Topics and Outcomes until mapping is complete.

Entering Criteria



Enter Criteria

2014 CAE 4YR SUBMISSION PROGRESS
SANDBOX UNIVERSITY

Step 1: Enter Course(s)

Edit/Add Courses — There are currently 1 active courses for Sandbox University

Step 2: Identify KUs and FAs

Identify KU — Edit the Knowledge Units your Institution intends to include in this cycle.

Identify FA — Add the Focus Areas your Institution intends to include in this cycle.

Step 3: Map KUs and FAs using the tables below.

Step 4: Submit Application

Submit CAE IA/CD 4Y — All items in Step 3 must be completed before submitting the application.

Legend

	An (In Progress icon) will appear next to Units that have started.
✔	A ✔ (Completed icon) will appear next to Units that are completed.

Progress	Program Criteria	Action
	CAE IA/CD	Start

Progress	Knowledge Units (KUs)	Action
	Basic Data Analysis	Start
	Basic Scripting	Start
	Cyber Defense	Continue
	Cyber Threats	Start
	Databases	Start
	Fundamental Security Design Principles	Start
	IA Fundamentals	Start
	Intro to Cryptography	Start
	IT System Components	Start
	Network Defense	Start

Criteria List (4 yr)

2014 CAE MEASUREMENT CRITERIA
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List

Legend

✔	You will see the ✔ (checkmark icon) next to Criteria that have been answered.

Criteria

Expand All | Collapse All | Display CAE Application

- ⊞ 0. Letter of Intent
- ⊞ 1. Outreach/Collaboration
- ⊞ 2. Center for IA/CD Education
- ⊞ 3. A Robust and Active IA/CD Academic Program
- ⊞ 4. IA/CD is Multidisciplinary Within the Institution
- ⊞ 5. Practice of IA Encouraged Throughout the Institution
- ⊞ 6. Student-based IA/CD/Cybersecurity research
- ⊞ 7. Number of IA/CD/Cybersecurity faculty and course load.
- ⊞ 8. Faculty active in current IA/CD/Cybersecurity practice and research.

Expanded Criteria

2014 CAE MEASUREMENT CRITERIA
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List

Legend

✔	You will see the ✔ (checkmark icon) next to Criteria that have been answered.

Criteria

Expand All | Collapse All | Display CAE Application

⊟ **0. Letter of Intent**

Answered	Category
	0. Letter of Intent **(Point Value: 0)**

⊟ **1. Outreach/Collaboration**

Answered	Category
	a. Shared curriculum **(Point Value: Up to 5 points/3 points required)**
	b. Reciprocity of credits **(Point Value: Up to 5 points/3 points required)**
	c. Sponsorship of or participation in Cyber Defense or Forensics Exercises and competitionwithin 3 years of submissions **(Point Value: Up to 5 points)**
	d. CAE Collaboration **(Point Value: Up to 5 points)**
	e. Community Outreach **(Point Value: Up to 5 points)**

⊞ **2. Center for IA/CD Education**

⊞ **3. A Robust and Active IA/CD Academic Program**

Criteria List (4 yr)

2014 CAE MEASUREMENT CRITERIA
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List

Legend

✔	You will see the ✔ (checkmark icon) next to Criteria that have been answered.

Criteria

Expand All | Collapse All | Display CAE Application

- ⊞ 0. Letter of Intent
- ⊞ 1. Outreach/Collaboration
- ⊞ 2. Center for IA/CD Education
- ⊞ 3. A Robust and Active IA/CD Academic Program
- ⊞ 4. IA/CD is Multidisciplinary Within the Institution
- ⊞ 5. Practice of IA Encouraged Throughout the Institution
- ⊞ 6. Student-based IA/CD/Cybersecurity research
- ⊞ 7. Number of IA/CD/Cybersecurity faculty and course load.
- ⊞ 8. Faculty active in current IA/CD/Cybersecurity practice and research.

Return to CAE IA/CD Progress List

All Criteria Completions Use Same Format: “http:// links, pdf uploads, and/or keyb”

ADD SELECTED CAE CRITERIA
SANDBOX UNIVERSITY

Selected Criteria

7. Number of IA/CD/Cybersecurity faculty and course load.
The institution must demonstrate that IA/CD faculty consists of a sufficient number of full time IA/CD faculty members and additional faculty members (may be part-time, adjunct, visiting professor, etc.) teaching at least one IA/CD course. This criterion requires a link to a biography or curriculum vitae for each faculty member.

(Overall Point Value: 8 Minimum/16 Maximum)

b. Identify by name additional full-time IA/CD faculty members
Identify by name additional full-time IA/CD faculty members (not listed in 7.a.), teaching IA/CD courses within the department that sponsors IA/CD programs. Provide link to biography or CV.

(2 points each/6 points maximum)

Note: **Bold*** items below are required.

Add Up to 5 Link(s)

All Links Must begin with "http://" or "https://".

Link 1

Link 2

Link 3

Link 4

Link 5

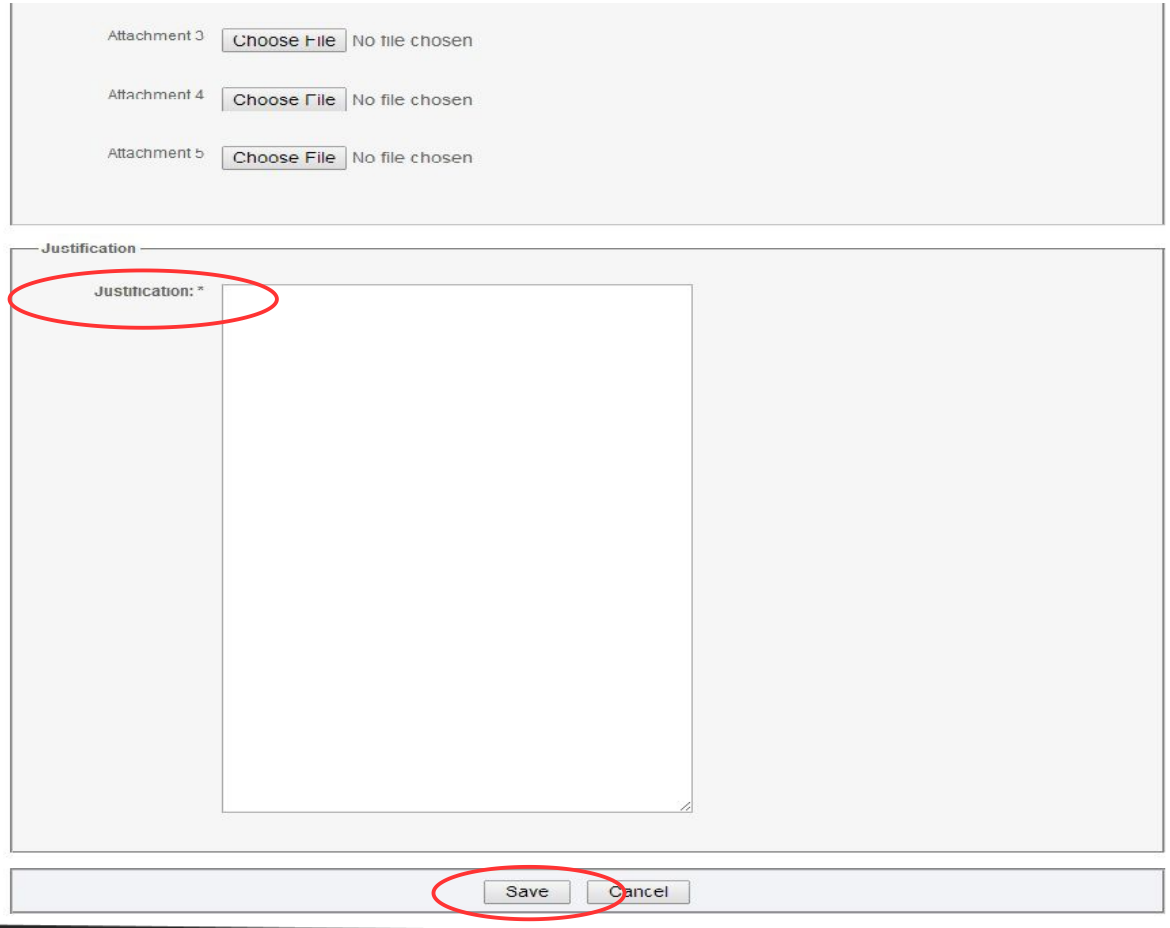
Add Up to 5 Attachment(s)

Only PDF files may be uploaded. Please virus scan any attachment prior to uploading.

Attachment 1 Choose File No file chosen

Attachment 2 Choose File No file chosen

All Criteria Completions Use Same Format: “http:// links, pdf uploads, and/or keyb”



Identification of Entered Elements

2014 CAE MEASUREMENT CRITERIA
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List

Legend

✔	You will see the ✔ (checkmark icon) next to Criteria that have been answered.

Criteria

Expand All | Collapse All | Display CAE Application

0. Letter of Intent

Answered	Category
	0. Letter of Intent **(Point Value: 0)**

1. Outreach/Collaboration

Answered	Category
✔	a. Shared curriculum **(Point Value: Up to 5 points/3 points required)**
	b. Reciprocity of credits **(Point Value: Up to 5 points/3 points required)**
	c. Sponsorship of or participation in Cyber Defense or Forensics Exercises and competitionwithin 3 years of submissions **(Point Value: Up to 5 points)**
	d. CAE Collaboration **(Point Value: Up to 5 points)**
	e. Community Outreach **(Point Value: Up to 5 points)**

Criteria List

2014 CAE MEASUREMENT CRITERIA
SANDBOX UNIVERSITY

Return to CAE IA/CD Progress List

Legend

✔	You will see the ✔ (checkmark icon) next to Criteria that have been answered.

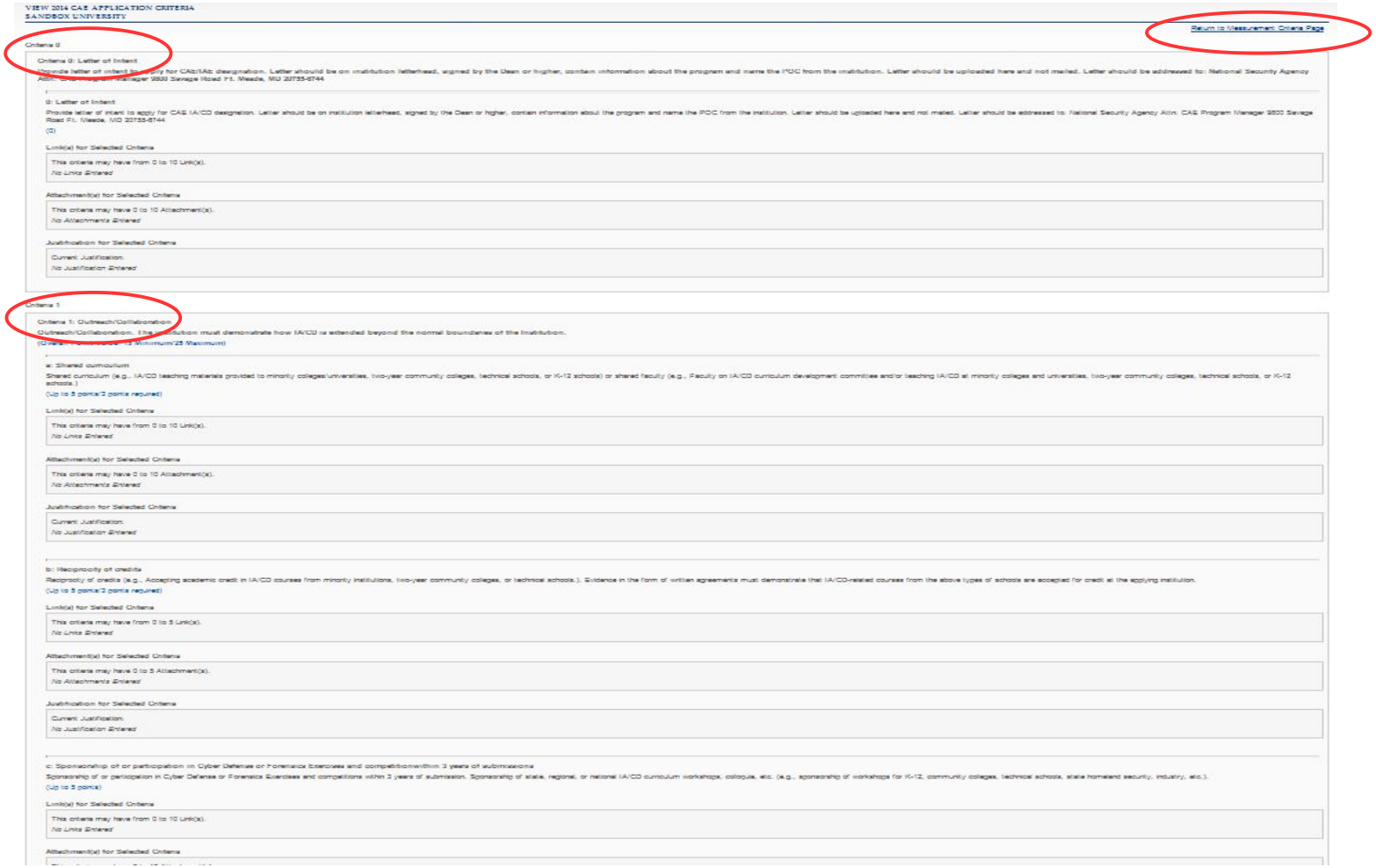
Criteria

Expand All | Collapse All | Display CAE Application

- ⊞ 0. Letter of Intent
- ⊞ 1. Outreach/Collaboration
- ⊞ 2. Center for IA/CD Education
- ⊞ 3. A Robust and Active IA/CD Academic Program
- ⊞ 4. IA/CD is Multidisciplinary Within the Institution
- ⊞ 5. Practice of IA Encouraged Throughout the Institution
- ⊞ 6. Student-based IA/CD/Cybersecurity research
- ⊞ 7. Number of IA/CD/Cybersecurity faculty and course load.
- ⊞ 8. Faculty active in current IA/CD/Cybersecurity practice and research.

Return to CAE IA/CD Progress List

Criteria Content



Sample Letter of Intent

ROSE STATE COLLEGE — OFFICE OF THE PRESIDENT

January 12, 2010

Ms. Christine Nickell
National Security Agency
9800 Savage Road, Suite 6744
Fort Meade, MD 20755-6744

Dear Ms. Nickell:

Please accept this letter as administrative endorsement of the Rose State College (RSC) effort to apply for the Center for Information Assurance Education and Training (CAE2Y/IAT) designation for two-year institutions. The College is committed to computer security and to achieving the CAE2Y certification sponsored by the National Security Agency and the Department of Homeland Security. RSC has made significant progress in the information security arena, and the College appreciates your guidance and assistance in preparing for the application process.

As an institution accredited by the Higher Learning Commission of the North Central Association since 1970, Rose State is committed to the long-term success of a computer security education and training program which will provide unique educational preparation for RSC students to enter the workforce in this field. Rose State College faculty and administration were successful in the mapping process. As a result, faculty received the award for RSC's successful efforts to map to 4011, 4012, 4013, 4014, 4015, and 4016 standards. Rose State College will be proud to attend the Colloquium for Information System Security Education in June 2010 to receive the CAE2Y designation.

Rose State College has encouraged its staff to move forward with this project. Mr. Kenneth Dewey from the Business and Information Technology Division will be coordinating the CAE2Y/IAT application. He is doing so with the approval and support of Mr. Arthur Zenner, Dean of the Business Information Technology Department; Dr. Frances Hendrix, Vice President for Academic Affairs; and myself, Dr. Terry Britton, President of Rose State College.

Sincerely,

Terry Britton

Terry Britton

(405) 733-7300
(405) 733-7399

S.E. FIFTEENTH
MIDWEST CITY
OKLAHOMA

- **http://www.rose.edu/Websites/rose2010/Images/Academics/Business%20and%20IT/Networking/CAE2Y/RoseStateCollegeCAE2YLetterofInternet.PDF**

Examples of Previous Criteria

Hagerstown CC

http://www.cssia.org/userfiles/files/Criteria%20For%20Measurement%20CAE2Y%20-%20HagerstownCC.pdf

Inver Hills CC

http://www.docstoc.com/docs/142155000/Inver-Hills-Community-College---cssia

Oklahoma CareerTech

http://www.okcareertech.org/about/initiatives/cyber-security/cae2y/cae2y-application

Richland College

http://www.cssia.org/userfiles/files/richland%20college%20cae2y%20application.pdf

Rose State College

http://www.cssia.org/userfiles/files/RSC%20CAE2Y%20Application.pdf

Resources

- CAE Program Office
  - askcaeiae@nsa.gov
- The National CyberWatch Center
  - http://www.cyberwatchcenter.org/
- Fred Klappenberger
  - faklappenberger@gmail.com
- Cyber Watch West
  - Corrinne Sande, Director/PI CyberWatch West
  - csande@whatcom.ctc.edu
- The Center for Security and Information Assurance
  - Susan Sands susands@sbcgobal.net

"On behalf of the entire staff, let me thank you for breaking up that meeting."