2 CAE & CAE2Y RESOURCES

The changes to the CAE process in the last year have caused concern and apprehension among current CAEs and potential new applicants. These concerns center on the new knowledge units (KUs) that replaced the CNSS mapping standards and the review process which now includes the site visit. The CNSS standards that have been used for the past 15 years as the requirement for the eligibility for an institution to apply for the CAE designation have been widely criticized as time consuming, obsolete, not necessary, etc. The CNSS standards have been replaced with KUs that are NOT a prerequisite to the CAE application, but an integral part of the CAE application. While this is a welcome change, the new CAE application process, the lack of familiarity with the new KU mapping has generated a lot of anxiety.

2 Recently, the National CyberWatch Center (NCC) started a webinar series designed to address these concerns. On January 31st, the first webinar titled CAE: Onboarding and Renewing described the CAE, covered the benefits of the CAE designation for institutions, explained the program requirements and provided an introduction to the mapping process.

The fact that 129 faculty registered for this webinar attests to the interest in these issues and the persistent need for additional explanation and support. NCC is offering three webinars in the next two months to address the different parts of the CAE application process and answer questions raised.

2 Presenters in the webinars include Casey O'Brien, the PI and Director of the National CyberWatch Center, Fred Klappenberger, who developed the first CyberWatch curriculum in cybersecurity and has completed the CNSS mapping process himself, Denisha Jackson the NSA National CAE2Y Program Manager National IA Education and Training Program and Vera Zdravkovich, who has been instrumental in establishing the CAE2Y designation.

The National CyberWatch Center offers different resources to support the CAE2Y community. In addition to the Webinar Series, resources include:

The NCC website has several CAE2Y applications posted. While these were completed under the old application process, the criteria are very similar, and these applications may be very helpful especially to the new applicants.

Personal Assistance

Dr. Fred Klappenberger is the NCC KU and CAE2Y consultant and can be contacted in case of additional questions/concerns. Dr. Vera Zdravkovich can assist with the criteria that are a part of the CAE2Y application process.

(e-mail address: tkepner@cyberwatchcenter.org

The first annual Community College Cyber Summit (3CS) will be held July 21 and 22, 2014, at the National Resource Center for Systems Security and Information Assurance (CSSIA), Moraine Valley Community College, Palos Hills, Illinois, a half-hour drive southwest of Chicago. 3CS will be an add-on to the High Impact Technology Exchange Conference (HI-TEC), and will take place during the HI-TEC pre-conference workshops. The Summit focuses on the cybersecurity education. A pre-conference KU workshop will offer hands-on instruction and assistance with the KU mapping.

The NCC is in the process of preparing a CAE2Y application process guide to provide additional assistance.

The following CAE Webinars @ 11 AM EST.

- **March 14th //** will be a Question and Answer session for those institutions ONLY which are re-designating under the new CAE requirements. You can register and submit your questions at http://goo.gl/xHJiX3
- **March 21st //** for institutions NEW to the CAE application process. Topics will include Getting Started, Identifying Criteria, and Demonstration of the Mapping Process in addition to a Question and Answer opportuntiy. You can register at http://goo.gl/14pGnY
- **April 4th //** will be a Question and Answer session for the institutions NEW to the CAE application process. Participants will be invited to submit their questions on the designated site.

The CAE2Y designation brings attention and respect to the program and the institution and elevates opportunities for additional funding. With all the resources described here, there is no reason for a community college not to invest the time and effort to apply for this valuable institutional designation.

CAE2Y.NEWS

Lead Investigator :: Vera Zdravkovich // Editor :: Teri Kepner // Designer :: Dan Slater
Volume 2 // Issue 1 // CAE2Y Newsletter // **March 2014**
Center for Academic Excellence 2-Year

NSF ATE Cybersecurity Centers	CyberWatch Maryland cyberwatchcenter.org	CyberWatch West California cyberwatchwest.org	CSSIA Illinois cssia.org	CSEC :: OK cseconline.org

NEW! Volume Two **March 2014**

2010 CAE2Y INSTITUTIONS ::

Anne Arundel Community College* - *Maryland*

Hagerstown Community College* - *Maryland*

Moraine Valley Community College - *Illinois*

Oklahoma City Community College - *Oklahoma*

Prince George's Community College* - *Maryland*

Rose State College - *Oklahoma*

2011 CAE2Y INSTITUTIONS ::

College of Southern Maryland* - *Maryland*

Community College of Baltimore County* - *Maryland*

Erie Community College* - *New York*

Inver Hills Community College* - *Minnesota*

Owens Community College - *Ohio*

Richland College* - *Texas*

Whatcom Community College* - *Washington*

* NATIONAL CYBERWATCH CENTER MEMBER

2012 CAE2Y INSTITUTIONS ::

Bossier Parish Community College - *Louisiana*

Frances Tuttle Technology Center - *Oklahoma*

Harford Community College* - *Maryland*

Ivy Tech Community College* - *Indiana*

Jackson State Community College - *Tennessee*

Minneapolis Community and Technical College - *Minnesota*

Montgomery College* - *Maryland*

Oklahoma Department of Career and Technology - *Oklahoma*

Sinclair Community College* - *Ohio*

Snead State Community College - *Alabama*

Valencia College* - *Florida*

2013 CAE2Y INSTITUTIONS ::

Blue Ridge Community and Technical College* - *West Virginia*

Florida State College at Jacksonville - *Florida*

Highline Community College - *Washington*

Honolulu Community College - *Hawaii*

Howard Community College* - *Maryland*

Manhattan Area Technical College - *Kansas*

Northern Virginia Community College* - *Virginia*

San Antonio College- *Texas*

St. Philip's College- *Texas*

***This newsletter is produced by the National CyberWatch Center**, an ATE center supported by a National Science Foundation grant with Prince George's Community College as the lead institution.*

PRINCE GEORGE'S COMMUNITY COLLEGE

NSF

2014 National Cyberwatch Center Webinar Series

- **>> March 28** // Conducting Classroom-Based Research
- **>> April 25** // National Cybersecurity Student Association
- **>> May 30** // National Cybersecurity Workforce Framework 2.0
- **>> August 29** // National Cyber League (NCL) for the College Classroom
- **>> Sept. 26** // Security Clearances
- **>> Oct. 31** // Critical Skills for Industry and Government
- **>> Nov. 21** // Building Enrollments

1 CAE Mapping for Re-Designation – Moving from CNSS to KU

Yes, it's true: a new CAE in IA/CD designation replaces the previous CAE in IA. All institutions are being strongly encouraged to transition to the new designation by December 2014. NSA has published a schedule for current CAEs to apply for re-designation. It can be found at http://www.cisse.info/pdf/2014/2014%20CAE%20Designation%20Schedule.pdf.

1 In the new system, Knowledge Units (KUs) replace the CNSS standards of the original CAE requirements. KUs are relatively tightly targeted technology areas composed of a set of topics and expected outcomes. They are the fundamental building blocks (think Legos) upon which the CAE in IA/CD rests. While a set of nearly 70 KUs replaces (and goes beyond) the seven CNSS standards of the original CAE requirements, fewer than two dozen KUs need be referenced by four year institutions and less than a dozen by community colleges to meet minimum mapping requirements for CAE designation. Specifically, a fixed set of eleven Core KUs make up the foundation of all mappings. Community colleges must map to all eleven of them. Four year institutions must map to those eleven Core KUs, plus an additional prescribed set of six, plus five more optional ones that may be chosen from a set of 51. [Check lists of all the Mandatory KUs and all Optional KUs are available from the Colloquium for Information Systems Security Education (CISSE)]

NSA/DHS has developed and made available a document titled, 2014 CAE KU Mapping Matrix, to facilitate an institution's data gathering in support of mapping. This is an especially useful tool. It consists of a main sheet **(Fig. 1)** displaying the hot-linked names of all Core and Mandatory KUs. The KUs are grouped into two year, four year, and optional categories.need to align to the KUs.

Clicking on the name of any KU on this sheet brings up the topics and expected outcomes for that KU onto which course mappings can be done **(Figs. 2 and 3).** Consider the structure of the simplest KU, Basic Data Analysis. It consists of only four topics: Summary Statistics, Graphing/Charts, Spreadsheet Functions, and Problem Solving.

1 Toss in the expected outcome: "Student will be able to apply standard statistical inference procedures ..." and the KU is completely defined.It is the job of each institution to specify how those topics will be met and how the outcome will be measured. Even though other KUs have more topics and more expected outcomes, their designs are all the same, i.e. list of topics and series of expected outcomes. **See Fig. 3** as another example of the similarity structure.

FIGURE 02 Basic Data Analysis KU

	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		

1 Columns A, B, and C contain the KU's structure. In columns D, E, … of row 1, institutions insert course designations which are being mapped to KU topics.

Institutions that have previously mapped to the CNSS standards will find the KU mapping process familiar: i.e, a KU topic is matched to the course(s) in which it is covered. Initially, an "X" is placed in any cell which is the intersection of a KU topic and a course component. **See Figs 4 and 5.**

FIGURE 01 Main Sheet - 2014 CAE KU Mapping Matrix

	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	

FIGURE 03 Basic Scripting KU

	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		

FIGURE 04 Basic Data Analysis KU "X'd

	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	

FIGURE 05 Basic Scripting KU "X'd

	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

In subsequent iterations the cells containing "Xs" are widened to accept references to specific course elements as in an identified textbook, course outline, handout, lab, etc. which covers the topic. Outcomes validation should also be mapped in their respective course cells with statements specifying what test instrument(s) will be used **(Fig. 6).**

FIGURE 06 Basic Scripting KU Mapped

	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

Once all individual content experts' contributions have been gathered and merged for the requisite KUs, culled to remove redundancy, and mapped into the spreadsheet, the spreadsheet becomes the source document for entering data into the NSA/DHS database.

For some topics, a printout of the previous (CNNS) mapped spreadsheet might be used as a aid to match topics with course content. However, KUs tend to be more detail oriented than CNSS standards. For example, the CNSS listed three topics within Cryptography, but the replacement KU consists of ten. Similarly, CNSS had no separate category for Systems Administration, but there is a Core KU addressing that area with 16 topics. In brief, there's no straightforward translation from CNNS to KU mapping. Nonetheless, institutions reapplying have the advantage of having prior practical experience with the mapping process. Additionally, since the KU topic specificity is considerably more detailed and precise, institutions will find that the vagueness and guesswork frequently associated with previous CNSS topics has been eliminated.

TO SUMMARIZE:

1. Download and review reference materials available on CISSE at http://www.cisse.info/news/cae-certification
2. Identify the CAE level for which your institution plans to apply and the required KUs,
2. Using the 2014 CAE KU Mapping Matrix downloaded from CISSE, remove or hide all KU sheets except those needed for your institution's application. In other words, create a multi-sheet spreadsheet consisting only of the Core KUs (and optional ones, if applicable). Make the spreadsheet available under a tool such as Google Drive, Microsoft OneDrive, or iCloud to facilitate collaboration of content experts,
3. Enter relevant course designations across columns,
4. Have content experts map course elements and outcome verification to KU for every relevant course,
5. If a collaborative environment has not been used, merge all contributions into a single spreadsheet (eliminate redundancies), and
6. Enter the data from the spreadsheet into the NSA/DHS data base.

The National CyberWatch Center site (http://www.cyberwatchcenter.org/) offers assistance to mapping questions submitted to the following e-mail address: tkepner@cyberwatchcenter.org.