**DECIPHERING FEDERAL Guidelines**

**for CYBERSECURITY WORKFORCE**

**DEVELOPMENT**

**and**

**Mapping ISSA Series Content**

**OUTLINE**

1. Introduction
2. Mapping ISSA Series Content to Federal Guidelines
   1. ISSA Curriculum Mapping - CAE IA/CD Knowledge Units and Focus Areas
   2. ISSA Curriculum Mapping - NICE Cybersecurity Framework Categories and Specialty Areas
3. Summary
4. Appendix: Current Cybersecurity Workforce Initiatives
   1. National Centers of Academic Excellence (CAE)
      1. Curriculum Mapping Requirements for CAE IA/CD Designation
      2. CAE IA/CD Mapping Components
         1. Core Knowledge Units
         2. Optional Focus Areas
      3. Current Status
   2. National Initiative for Cybersecurity Education (NICE)
      1. Cybersecurity Workforce Framework
         1. Cybersecurity Workforce Framework Components
         2. Using the Cybersecurity Workforce Framework
      2. National Initiative for Cybersecurity Careers and Studies (NICCS)
         1. Cybersecurity Training and Education Catalog
         2. Mapping to the Workforce Framework
         3. Using the NICCS Tools and Resources
      3. Current Status
   3. Department of Defense Cybersecurity Workforce Development
      1. DoD Cybersecurity Workforce Framework
      2. DoDD 8570.01, Information Assurance Training, Certification and Workforce Management
      3. Current Status
5. Glossary of Terms/Acronym List

**I. INTRODUCTION**

The cybersecurity workforce is one of the most critical employment sectors in the country, and Jones & Bartlett Learning is committed to improving this workforce’s training and development. The nation’s cybersecurity is threatened by a wide array of hostile actors who seek to sabotage the U.S. information technology infrastructure—and thus our ability to compete in the global economy. No one is safe from this threat—not government, not private organizations, not individuals. For years it has been clear that the nation lacks an adequately trained and skilled workforce with the knowledge, skills, and abilities to meet the demand for cybersecurity workers. Establishing a more secure cyberspace requires improvement in many areas, among them developing a cybersecurity workforce that can get the job done.

Several government agencies have made overlapping efforts to develop standard guidance on the skills required for this evolving profession. Jones & Bartlett Learning has tackled head-on the challenge that training and education providers face in mapping cybersecurity training to multiple sets of federal government guidelines.

To better serve our customers and promote the strengthening of computer security, Jones & Bartlett Learning recently launched an analysis of federal government cybersecurity guidance documents. The objective was to identify the cybersecurity skills to which our curriculum uniquely maps and provide customers with the following added value:

* To help our customer base of academic institutions meet government training and development standards
* To demonstrate what students will have studied after completing a course
* To help students understand which cybersecurity skills employers are seeking
* To identify gaps in training the cybersecurity workforce, as well as trends requiring updating or supplementing of our courseware on a continuing basis

To prepare for our cybersecurity curriculum-mapping project, we surveyed the landscape of workforce development guidelines. In doing so, we sought an understanding of significant government cybersecurity workforce initiatives and their objectives, structure, and target audiences. As our customers have experienced, we found it a daunting task to wade through all the detailed documentation, make sense of it, and determine which guidelines are best suited to which target audience.

This paper is the result of those efforts. It provides background information on the relevant cybersecurity training, education, and workforce requirements. It provides a concise overview and the current status of each. Where applicable, it outlines how courses in Jones & Bartlett Learning’s Information Systems Security and Assurance (ISSA) series map to the following documents:

* National Centers of Academic Excellence (CAE)/Cyber Defense Education Program
* National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
* Department of Defense Cybersecurity Workforce Development Framework

The chart below provides a snapshot of the documents and sets the tone for understanding the challenge.

|  |  |  |  |
| --- | --- | --- | --- |
| **Comparison of**  **Federal Cybersecurity Workforce Guidelines** | | | |
|  | **CAE Program** | **NICE Workforce Framework** | **DoD CWF** |
| **Goal/ Objective** | Promotes higher education and research; and produces professionals with information assurance (IA) expertise in various disciplines | Describes and categorizes cybersecurity work and identifies sample job titles, tasks and KSAs | Provides the foundation for identifying education, training, and certification requirements to support cybersecurity personnel qualification |
| **Audience** | * 2-year, 4-year and graduate-level institutions in the U.S. seeking CAE designation * students, employers, and hiring managers | * colleges * training vendors * students * employers/employees * policymakers | * military, civilian, and contractor cybersecurity personnel * training vendors, certification bodies, colleges, and continuing education providers |
| **Mapping**  **Components** | * 2Y Core Knowledge Units * 4Y Core + Optional | * 7 Categories * 31 Specialty Areas * Task/KSA level * Job Titles | * DoD work roles, tasks, functions and baseline KSAs * Under Development |
| **Integration** | The NICE Framework informed development of the CAE Knowledge Units (KUs); thus, many CAE Core KUs are core across the NICE Framework Specialty Areas. NICE Framework will also inform development and implementation of the DoD CWF. | | |
| **Important Dates** | * CAE re-designation required by December 2014 * JBL maps will available to CAE customers January 2015 | * Version 2.0 released May 2014 * NICCS Cybersecurity Training Catalog now open to all training providers | * Currently under development; no target date available * 8570.01 to be revised * JBL will monitor DoD initiatives in 2014 |

1. **MAPPING THE ISSA SERIES TO FEDERAL REQUIREMENTS**

After reviewing current federal cybersecurity workforce initiatives, Jones and Bartlett Learning mapped the ISSA curriculum to the CAE IA/CD k. The logical place to begin our mapping exercise was to the CAE KUs, since the NICE Framework influenced development of the CAE Knowledge Units (KUs), and the DoD Cybersecurity Workforce Development Framework will also consider the NICE Framework.. Jones & Bartlett Learning will continue to monitor development of the DoD CWDF and map appropriate components to ISSA courses ([www.issaseries.com](http://www.issaseries.com)) as necessary in the future. Additionally, we are reviewing efforts to map to the NICE Framework.

Our goal was to help our customers, whether colleges and universities or technology training providers, identify the cybersecurity workforce skills to which our ISSA curriculum uniquely maps. We also wanted to ease the burden of meeting government mapping standards. Our ISSA course mappings thus add value in the following ways:

1. They support CAE institutions in meeting CAE KU mapping requirements for CAE IA/CD designation. Since the CAE structure focuses on the knowledge requirements of academic course content, we will provide each customer with a completed KU Mapping Matrix (in an Excel spreadsheet) for each ISSA course used in the customer’s curriculum for submission to the NSA CAE application website.
2. They facilitate training vendors’ submissions of ISSA courses mapped to the National Cybersecurity Workforce Framework. Once published in the NICCS Education and Training Catalog, courses will be visible to a nationwide audience, offering a marketing opportunity.
3. They promote courses identified by Specialty Area, Focus Area, tasks, or job title so that students and employees can more easily search for courses appropriate to their needs and career paths.

*NOTE: Jones & Bartlett Learning will refresh our cybersecurity course mappings on a regular basis as new textbooks, lab manuals, and courseware are completed*.

1. **ISSA Curriculum MapPING - CAE Knowledge Units and Focus Areas**

Jones & Bartlett Learning made it a priority to address the NSA/DHS Centers of Academic Excellence (CAE) IA/CD requirement to map to Core Knowledge Units (KUs). Our academic customers who are CAE-designated must meet the new curriculum-mapping requirements by the end of 2014. They must apply via the CAE IA/CD website for each course.

To facilitate our customers’ submission of all courses (Topics and Outcomes) to NSA’s online database, Jones & Bartlett Learning will provide a completed KU Mapping Matrix (Excel spreadsheet format) for each ISSA course. These will be promoted via our sales representatives, webinars, and marketing on <http://www.issaseries.com>.

1. **ISSA Curriculum - KU Mapping Matrix**

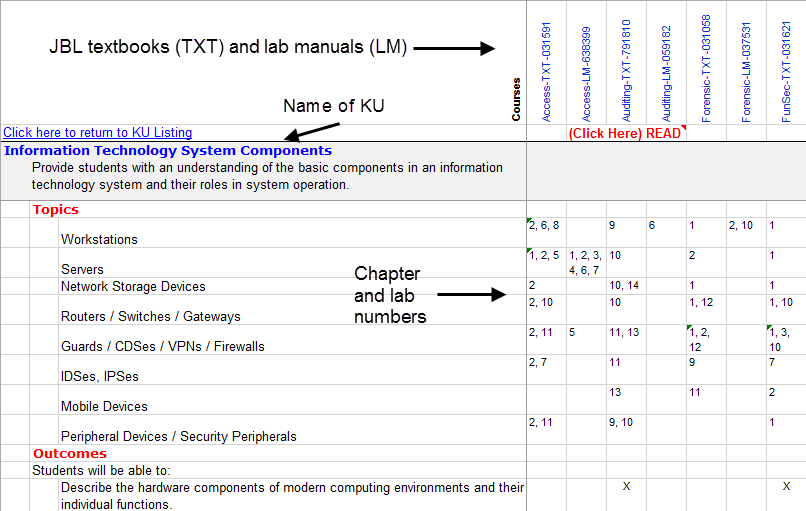
The basic features of all CAE Knowledge Units, Core and Optional, are Topics, Outcomes and Courses. A minimum list of Topics to be covered and one or more Outcomes, or learning objectives, is required.

CAE Core 2Y and Core 4Y KUs were mapped to the 13 courses in the ISSA curriculum:

* Access Control, Authentication, and Public Key Infrastructure
* Auditing IT Infrastructure for Compliance
* Systems Forensics, Investigation and Response
* Fundamentals of Information Systems Security (online course title: Introduction to Information Systems Security)
* Hacker Techniques, Tools, and Incident Handling
* Legal Issues in Information Security
* Security Strategies in Linux Platforms and Applications
* Network Communications Infrastructure
* Network Security, Firewalls, and VPNs
* Security Policies and Implementation Issues
* Managing Risk in Information Systems
* Security Strategies in Web Applications and Social Networking
* Security Strategies in Windows Platforms and Applications

CAE Core 2Y and Core 4Y KU Topics are mapped primarily to course textbook chapters and lab manual labs in which the topic is at least fully described. Some topics, however, are mapped to classroom discussions, the course syllabus, presentations, and other activities. The Outcomes are tied to measurable activities, so we mapped to graded discussions, graded assignments, labs, and course projects that measure each outcome. Our ISSA Mapping Matrix supports the offline data-gathering phase—identifying KUs that are to be mapped, then gathering and recording supporting course data, entering citations such as textbook, chapter, and page numbers.

**SAMPLE of CAE KU Matrix with JBL ISSA Course Mapping**



Textbooks are indicated in the column headings by <*course abbreviation*>-TXT-<*ISBN*>. That means the first textbook listed in Figure 2 is for the Access Control, Authentication, and Public Key Infrastructure (Access) course. Lab manuals follow the same convention but include “LM” in the column heading. Numbers that appear in the TXT and LM columns within the Topics sections refer to textbook chapter numbers and lab numbers, respectively. Specific graded activities are listed by name in the Outcomes sections in spreadsheets for individual courses; the combined spreadsheet (shown above) lists only Xs in the Outcomes section.

All Topics must be mapped.

Jones & Bartlett Learning will provide custom maps for Optional and Focus Area KUs upon request. Sales representatives will consult with individual schools to assess the Optional and Focus Areas best suited to each school’s curriculum and areas of interest.

The following Core KUs do not fully map to the JBL ISSA curriculum:

* Basic Data Analysis
* Basic Scripting
* Database Management Systems
* Probability and Statistics
* Programming

We have listed JBL textbooks that schools can adopt to fill in content gaps.

1. **ISSA Curriculum MapPING – NICE CYBERSECURITY workforce FRAMEWORK categories and specialty areas**

The NICE Framework describes cybersecurity work and the tasks within Specialty Areas. Example job titles are provided to assist students and potential employees in identifying career interests or career pathways. The NICE Framework focus on the work function is at a higher level than the new CAE structure, which focuses on knowledge requirements of academic course content at the Topic and Outcomes level. Beyond the release of the NICE Framework Version 2.0, an appropriate mapping of the Framework components to the NSA CAE Knowledge Units and Focus Areas should lead to a better understanding of how each program relates to the other. (An academic effort is currently underway to identify an appropriate procedure for this mapping.)

Now that the NICCS Education and Training Catalog is open to private sector training vendors, Jones and Bartlett Learning is establishing a process for mapping the 13 ISSA courses to the Framework Specialty Areas and appropriate Proficiency Levels. Once this effort is complete, we will make the information available to our training vendor customers to support their efforts in becoming NICCS Training Providers. The NICCS Education and Training Catalog will be a useful marketing tool for cybersecurity training vendors--upon publication, your courses will be visible to a nationwide audience. Publication in the NICCS Training Catalog will expose your courses to student and employees looking for courses to improve their skills and assist with career path opportunities.

1. **SUMMARY**

This paper outlines our analysis of federal government cybersecurity guidance documents and how Jones & Bartlett Learning has mapped its Information Systems Security and Assurance (ISSA) curriculum, having in mind three sets of federal government cybersecurity workforce guidelines:

* the National Centers of Academic Excellence (CAE)/Cyber Defense Education Program
* the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CWF)
* the Department of Defense Cybersecurity Workforce Development Framework (CWDF)

Each is aimed at a slightly different audience. The CAE is targeted at two-year and four-year academic institutions, as well as students, employers, and hiring managers. The NICE Framework aims at colleges, training vendors, students, employers and policymakers. The DoD CWDF addresses the Department’s military and civilian employees and vendors, and any academic or training organization involved in preparing cybersecurity employees. (More detailed information on the three initiatives is available in the Appendix.)

Institutions seeking re-designation as CAEs must do so by December 2014. The updated NICE CWF Version 2.0 was released in May 2014. DoD has not set a target date for release of the CWDF.

Jones and Bartlett Learning’s ISSA curriculum has been mapped to the CAE IA/CD and next step is to map it to the NICE CWF. Resulting CAE and NICE CWF maps will be refreshed on a regular basis as new textbooks, lab manuals, and courseware are completed. We will continue to monitor development of the DoD CWDF and map appropriate components to ISSA courses as necessary in the future. Moreover, Jones and Bartlett Learning can create custom learning objects in support of institutions’ needs in multiple modalities.

1. **APPENDIX: CURRENT Cybersecurity Workforce INITIATIVES**
2. **National Centers of Academic Excellence (CAE-2Y, CAE, CAE-R, CAE-OP Designation)**

The National Security Agency (NSA) and Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Information Assurance (IA) Education programs for academic institutions. The goals of these programs are:

* To reduce the vulnerability of the national information infrastructure by promoting higher education and research in information assurance (IA)
* To produce a growing number of professionals with IA expertise in various disciplines.

All regionally accredited two-year, four-year, and graduate-level institutions in the United States can apply for designation as a Center of Academic Excellence (CAE). A new NSA/DHS Information Assurance/Cyber Defense (IA/CD) designation is being implemented to strengthen the program and distinguish the strengths of each CAE institution. This will benefit not only the CAE, but also students, employers and hiring managers nationwide.

Institutions wishing to gain CAE designation must map their curriculum to NSA/DHS academic requirements and meet program criteria, including outreach and collaboration, student development, multidisciplinary efforts, and student curriculum path and recognition.

Beginning in August 2013, all institutions currently designated as CAEs, as well as those striving for designation, are required to apply under the new CAE IA/CD program according to a schedule posted at <http://www.cisse.info/pdf/2014/2014%20CAE%20Designation%20Schedule.pdf>. The goal is to implement the new program by December 2014. NSA and DHS established quarterly reviews based on current CAE/IA designation years and other programmatic requirements. Institutions may apply ahead of this schedule, but may not be evaluated until their scheduled quarter.

1. **Curriculum Mapping Requirements for CAE IA/CD Designation**

The CAE requirement to map courses to Knowledge Units replaces the original requirement to map to the Committee on National Security Systems (CNSS) training standards. The intent in modifying the CAE academic requirements was to better reflect the state of evolution in the IA discipline since the original publication of the CNSS training standards.

1. **CAE IA/CD Mapping Components**

The CAE IA/CD academic requirements seek to meet defined sets of Knowledge Units (KUs) created for the academic community to inform curriculum building. The KUs are targeted technology areas including topics and expected outcomes. They represent an extensive set of 70 KUs replacing seven original CNSS requirements. (Details are provided at <http://www.cisse.info/news/cae-certification>). Mapping components consist of:

* core KU requirements for two-year institutions
* core KU requirements for four-year institutions
* optional KUs of institutional choice
* optional Focus Areas

1. **Core Knowledge Units**

The KUs are level-specific for two-year, four-year, and graduate-level institutions. They require the successful mapping of the institution’s curriculum within three categories: Core, Mandatory, and Optional (see charts below). Each KU includes a minimum list of required topics and one or more outcomes or learning objectives. The institution can demonstrate in many ways that a program meets or fulfills a Knowledge Unit: via the course syllabus, prerequisite course(s), prerequisite degree, student assignments, modules in a course/collection of courses, or certifications (CCNA, etc.). A single course may fulfill the requirements of several Knowledge Units. Minimum requirements are as follows:

* Two-year institutions must map to all 11 Mandatory Core 2Y KUs
* Four-year institutions must map to six Mandatory Core 4Y KUs, plus the Core 2Y KUs and an additional five Optional KUs selected by the institution from among 51 choices.

|  |  |
| --- | --- |
| **CAE Core Knowledge Units** | |
| **CAE 2-YEAR SCHOOLS: Core 2Y: 11 Mandatory KUs** | |
| **Basic Data Analysis**  **Basic Scripting**  **Cyber Defense**  **Cyber Threats**  **Fundamental Security Design Principles**  **Information Assurance Fundamentals** | **Introduction to Cryptography**  **Information Technology Systems**  **Components**  **Networking Concepts**  **Policy, Legal, Ethical & Compliance**  **System Administration** |
| **CAE 4-YEAR SCHOOLS: Core 2Y PLUS Core 4Y: 6 Mandatory KUs** | |
| **Database Management Systems**  **Network Defense**  **Network Technology and Protocols** | **Operating Systems Concepts**  **Probability and Statistics**  **Programming** |
| **PLUS: 5 Optional KUs** | |

|  |  |
| --- | --- |
| **4Y Institutions Must Select Five (5) Optional KUs** | |
| **Advanced Cryptography**  **Advanced Network Technology and Protocols**  **Algorithms**  **Analog Telecommunications**  **Basic Data Analysis**  **Basic Scripting/ Intro Programming (4Y)**  **Certification and Accreditation**  **Cloud Computing**  **Cyber Defense**  **Cyber Threats**  **Cybersecurity Planning & Management**  **Data Administration**  **Data Structures**  **Database Management Systems**  **Databases**  **Device Forensics**  **Digital Communications**  **Digital Investigations**  **Embedded Systems**  **Forensic Accounting**  **Formal Methods**  **Fraud Prevention and Management**  **Fundamental Security Design Principles**  **Hardware Reverse Engineering Hardware/Firmware Security**  **Host Forensics**  **IA Architectures**  **IA Compliance**  **IA Fundamentals**  **IA Standards**  **Industrial Control Systems**  **Intro to Cryptography**  **Intrusion Detection** | **IT Systems Components**  **Life-Cycle Security**  **Low Level Programming**  **Media Forensics**  **Mobile Technologies Network Administration**  **Network Defense**  **Network Forensics**  **Networking Concepts**  **Networking Technology and Protocols**  **Operating Systems Concepts**  **Operating Systems Hardening**  **Operating Systems Theory**  **Overview of Cyber Operations**  **Penetration Testing**  **Policy, Legal, Ethics, & Compliance Probability & Statistics**  **Programming**  **QA / Functional Testing**  **RF Principles**  **Secure Programming Practices**  **Security Program Management**  **Security Risk Analysis**  **Software Assurance**  **Software Reverse Engineering**  **Software Security Analysis**  **Supply Chain Security**  **System Administration**  **Systems Engineering**  **Systems Programming**  **Virtualization Technologies**  **Vulnerability Analysis**  **Wireless Sensor Networks** |

1. **Optional Focus Areas**

All CAEs may apply for one or more CAE IA/CD Focus Area designations. Focus Area designations allow an institution to differentiate its IA/CD program from others in the marketplace. A CAE might apply for such a designation for many reasons. First, Focus Areas (or specialty topics) assist students in identifying areas of interest and making informed decisions about their programs of study. Second, Focus Areas allow hiring managers to recruit from institutions more efficiently and find the skills needed for their line of business. Finally, Focus Area designation also fosters and encourages further strengthening of IA/CD focused education and deepening of research at US institutions.

For an institution to be awarded a Focus Area designation, its curriculum must:

* Successfully map to all of the KUs identified in the Focus Area
* Allow a student to reasonably complete the necessary course of study, including all KUs identified in the Focus Area
* Provide student certificates to those who complete the Focus Area course of study. Certificates must clearly identify the specific Focus Area achieved.

CAE Focus Areas are shown in the table below.

|  |  |
| --- | --- |
| **CAE Focus Areas (Optional)** | |
| **Cyber Investigations**  **Data Management Systems Security**  **Data Security Analysis**  **Digital Forensics**  **Health Care Security**  **Industrial Control Systems-SCADA Security**  **Network Security Administration**  **Network Security Engineering**  **Secure Cloud Computing** | **Secure Embedded Systems**  **Secure Mobile Technology**  **Secure Software Development**  **Secure Telecommunications**  **Security Incident Analysis and Response**  **Security Policy Development and Compliance**  **Systems Security Administration**  **Systems Security Engineering** |

**3. Current Status**

All institutions (both two-year and four-year) currently holding an NSA/DHS CAE designation in Information Assurance and/or Research must reapply for designation under the new CAE IA/CD Program by December 2014. This includes mapping courseware and content to the new Core KUs. There are no fees for the application. Institutions seeking first-time CAE designation can apply at any time and need not adhere to the Quarterly Designation Schedule referenced above.

The previous program, the CNSS Information Assurance Courseware Evaluation (IACE) program, allowed commercial training and education content providers to submit their curriculums for NSA evaluation, but the NSA has terminated it. Therefore, commercial training and education content providers are no longer included in the NSA/CAE evaluation team’s curriculum reviews.

1. **National Initiative for Cybersecurity Education (NICE)**

**The National Initiative for Cybersecurity Education (NICE)** is a nationally coordinated effort including more than 20 federal departments and agencies, academia, and industry.

**The goals of this initiative are to:**

* maintain a globally-competitive cybersecurity workforce
* broaden the pool of skilled workers able to support a cyber-secure nation.

**The NICE initiative is not limited to the federal workplace. It includes private industry, people changing careers, and students—from kindergarten through postgraduate school. It includes activities to examine and more clearly define cybersecurity workers’ various roles and responsibilities and to improve cybersecurity workforce training. The initiative aims to define the cybersecurity population consistently using standardized terms. It considers this an essential step in ensuring that the U.S. can educate, recruit, train, develop, and retain a highly qualified workforce.** To effectively coordinate the cybersecurity job market, colleges, educators, employers, employees, and training vendors need a standardized way to describe the work encompassed by the term *cybersecurity*.

**The National Cybersecurity Workforce Framework and the National Initiative for Cybersecurity Careers and Studies (NICCS) portal are among NICE resources of special interest to private sector training, education, and certification vendors.**

1. **Cybersecurity Workforce Framework**

The Cybersecurity Workforce Framework was developed as a national resource that categorizes, organizes, and describes cybersecurity work. It provides a systematic way for educators, students, employers, employees, training providers, and policymakers to organize the way they think and talk about cybersecurity work and workforce requirements. When degrees, jobs, training, and certifications are aligned to the Cybersecurity Workforce Framework:

* Colleges and training vendors can create programs aligned to jobs
* Students will graduate with knowledge and skills that employers need
* Employers will have a larger pool of more qualified candidates from which to recruit
* Employees will have more defined career paths and opportunities
* Policymakers can set standards to advance the field and promote job growth

The Framework **provides a classification system and common vocabulary for organizing cybersecurity work** and workers that share common major functions, regardless of actual job titles. These include the information technology, information assurance, and computer science populations. See <http://csrc.nist.gov/nice/framework/>. Among other benefits, this will allow organization to set salary ranges for comparable work.

* 1. **Cybersecurity Workforce Framework Components**

The Framework uses Categories and Specialty Areas to group similar types of work. Related Specialty Areas are grouped under the umbrella of a single Category. Each Specialty Area represents a function within the cybersecurity field. Typical tasks, knowledge, skills, and abilities (KSA) statements, and sample job titles define the work within each Specialty Area.

The Framework describes cybersecurity work regardless of organizational structures, job titles, or other idiosyncratic conventions. For example, an individual may perform tasks in more than one Specialty Area. Or, all an individual’s work may fall within a single Specialty Area. The Specialty Areas, made up of KSAs with associated tasks, can be overlaid onto any organization’s existing occupational structure, since the Framework describes cybersecurity work, tasks, and competencies based on their functions.

|  |  |
| --- | --- |
| **NICE Cybersecurity Workforce Framework** | |
| **CATEGORIES** | **SPECIALTY AREAS** |
| **Securely Provision** | *Secure Acquisition*  *Secure Software Engineering*  *Systems Security Architecture*  *Technology Research and Development*  *Systems Requirements Planning*  *Test and Evaluation*  *Systems Development* |
| **Oversee and Govern** | *Legal Advice and Advocacy*  *Strategic Planning and Policy Development*  *Training, Education and Awareness*  *Information Systems Security Operations*  *Security Program Management*  *Risk Management*  *Knowledge Management* |
| **Operate and Maintain** | *Data Administration*  *Customer Service and Technical Support*  *Network Services*  *System Administration*  *Systems Security Analysis* |
| **Protect and Defend** | *Enterprise Network Defense (END) Analysis*  *Incident Response*  *Enterprise Network Defense (END) Infrastructure Support*  *Vulnerability Assessment and Management* |
| **Analyze** | *All Source Intelligence*  *Exploitation Analysis*  *Targets*  *Threat Analysis* |
| **Collect and Operate** | *Collection Operations*  *Cyber Operations Planning*  *Cyber Operations* |
| **Investigate** | *Investigation*  *Digital Forensics* |

* 1. **Using the Cybersecurity Workforce Framework**

The Workforce Framework can be an important tool in building and maintaining a highly skilled and agile workforce because it provides the necessary structure and common language for standardizing the description of cybersecurity work. Benefits of having a common language include:

* Helping academic institutions and training providers develop relevant training for cybersecurity jobs
* Giving students and job candidates a better understanding of the skills needed for cybersecurity careers
* Providing employers with clear skill requirements to use for recruitment, selection, and workforce development
* Supporting policymakers who must set standards to promote workforce professionalization

1. **National Initiative for Cybersecurity Careers and Studies (NICCS)**

**DHS developed the National Initiative for Cybersecurity Careers and Studies (NICCS) as a central repository of cybersecurity resources. It is available to anyone who seeks to learn more about cybersecurity and opportunities in the field.** The repository is organized into a training catalog for easy search ability and access, including **training courses mapped to the Cybersecurity Workforce Framework. The NICCS portal also provides tools and resources for specific user groups.**

**a. Cybersecurity Education and Training Catalog**

The NICCS Cybersecurity Education and Training Catalog serves as a central repository where cybersecurity professionals can find courses needed to improve their skill set, increase their level of expertise, earn certifications, or even transition to new careers. The Catalog also offers cybersecurity vendors a marketing opportunity—upon publication, their courses will be visible to a nationwide audience.

DHS maintains the Catalog’s integrity through vetting criteria to ensure that the courses listed are offered by organizations recognized as providing quality resources. Therefore, only approved training providers may post courses. This requires the submission of data to DHS indicating that courses map to NICE Framework Specialty Areas. To submit courses to the Catalog, organizations must complete and submit a Vendor Vetting Form at <http://niccs.us-cert.gov/training/vendor-vetting-web-form>***.***

To ensure that each provider listed is a legitimate business, any provider seeking to publish courses in the Catalog must meet one of the following criteria:

* Designation as a National Center of Academic Excellence (CAE)
* Approval as a training provider by a federal agency or department
* Listing as an approved and valid vendor on the General Services Administration (GSA) schedule
* Accreditation by a body recognized by U.S. Department of Education or the Council for Higher Education Accreditation (CHEA) in the case of academic institutions
* Experience, including at least one year in business, delivery of the training course(s) at least twice over 18 months, and a business entity license.

**b. Mapping to the Workforce Framework**

Each course listed in the NICCS Cybersecurity Education and Training Catalog must be mapped to the Workforce Framework, and only approved training providers may post courses. The Catalog’s success depends on the completeness and accuracy of the information organizations provide. Users can more easily search for courses that meet their needs when they must review only courses mapped to the Framework and identified by Specialty Areas made up of KSAs and associated tasks.

To add training courses to the Catalog, providers must submit a completed NICCS Provider Template. They can obtain this by contacting the NICCS Supervisory Office at [NICCS@hq.dhs.gov](mailto:NICCS@hq.dhs.gov%20%20) and obtaining a NICCS Provider ID. Material is mapped to the overarching Specialty Areas. Following instructions on the forms, providers identify which Specialty Areas align to each training course and map up to five Specialty Areas to each course. They then select the appropriate training proficiency level. Once the provider has mapped the courses, it submits the training information the NICCS Supervisory Office.

**c. Using NICCS Tools and Resources**

The Framework’s success depends on user groups’ ability to easily and effectively promote, adopt, and use it. Tools and resources are provided to help use the Framework in government, academia, and the private sector. Customized user guides available on the NICCS website provide implementation guidance, useful tools, and links to promote the Framework’s use. Customized user guides are also available to provide various organizations with specific assistance in using and implementing it: employers, training vendors, academic institutions, and educators.

1. **Current Status**

DHS released a draft of the NICE Workforce Framework Version 2.0 in May 2014, but Version 1.0, dated March 2013, remains in effect as the primary resource for federal agencies. Working with the Office of Personnel Management, NICE will release a transition plan to Version 2.0 that will preserve the work federal agencies have completed to date.

Since many of the CAE Core Knowledge Units are also core in the Framework’s Specialty Areas, a **next logical step is for DHS to work with NSA in the near future to map the NICE Framework to the NSA CAE IA/CD requirements. This would allow everyone in the cybersecurity job market—colleges, educators, employers, employees, and training vendors—to use a standard description of the work covered by the term *cybersecurity.* The CAE IA/CD focuses on promoting higher education and producing more professionals with IA expertise in various disciplines. The Cybersecurity Workforce Framework describes and categorizes cybersecurity work functionally and identifies sample job titles, tasks and KSAs. Mapping the CAE KUs and Focus Areas to the NICE Specialty Areas would make it easier to develop consistent cybersecurity career paths—helping to create an academic foundation for the specific job and skills training needed to function effectively in the workplace.**

1. **DePARTMENT OF DEFENSE Cybersecurity WORKFORCE DEVELOPMENT**

The Department of Defense recently released a new DoD Cyberspace Workforce Strategy (DCWS). This enterprise strategy seeks to transform the military and civilian cybersecurity workforce, including training and retaining staff in a competitive national environment. The DCWS focuses on establishing workforce requirements and producing consistent and applicable cybersecurity skills and abilities. The DCWS workforce goals include:

* + promoting qualification and continuous learning
  + producing professionals with cybersecurity expertise in various disciplines

A key strategic effort is to set standards to identify cybersecurity work roles, qualifications, and parameters for managing the workforce. A critical element in the DCWS is development of a standard vocabulary for cybersecurity work roles, moving from IA personnel workforce policies to cybersecurity workforce policies with common work roles and qualifications for all cybersecurity positions. Additionally, in support of the diverse professional development requirements, the DoD cybersecurity workforce will need integrated learning in a variety of training environments, including:

* traditional classroom training
* virtual training
* hands-on laboratories
* realistic, operational exercises.

The DCWS intends to institutionalize continuous learning with greater focus on evaluating the maturity of cybersecurity skills. Shifting from static training and certification/qualification to dynamic, relevant continuous learning will facilitate developing and measuring proficiency.

1. **DoD Cybersecurity Workforce Development Framework**

The DoD Cybersecurity Workforce Development Framework (CWDF), now under development, will describe and categorize DoD cybersecurity work and identify specialty areas, roles, tasks and KSAs. It will also provide a basis for identifying education, training, and certification requirements to support personnel qualification. The DoD CWDF will be based on integrating the NICE Cybersecurity Workforce Framework and the Joint Cyberspace Training and Certification Standards to provide a vocabulary of work roles by specialty area—each with a baseline set of required KSAs—as well as functions.

1. **DoDD 8570.01 Information Assurance Training, Certification and Workforce Management**

New policies and directives will be developed and reconciled with exiting IA directives. For example, DoDD 8570.01, Information Assurance Training, Certification, and Workforce Management, addresses only the IA workforce. Since the CWF will identify all cyberspace workforce roles, existing policies will be replaced or broadened as needed for the entire cybersecurity workforce. This foundation will support DoD’s ability to implement proficiency measurements to plan for the cybersecurity workforce of the future.

1. **Current Status**

The DoD Office of the Chief Information Officer is currently developing the DoD CWDF with a working group of representatives from Department components. DoD has not currently set a target date.

To establish an integrated range of learning, additional components planned for development under the DoD CWS include:

* Institutionalizing proficiency development and measurement
* Identifying and leveraging DoD-wide training and education opportunities
* Establishing an environment fostering continuous learning and professional development
* Providing for individual and collective training in realistic simulated environments.

1. **GLOSSARY OF TERMS/ACRONYM LIST**

|  |  |
| --- | --- |
| CAE | National Center of Academic Excellence in Information Assurance Education |
| CAE-2Y | National Center of Academic Excellence, Two Year |
| CAE-OP | National Center of Academic Excellence, Cyber Operations |
| CAE-R | National Center of Academic Excellence, Research |
| Categories | Overarching structure of the NICE Framework; seven (7) Categories group Specialty Areas by job function |
| CD | Cyber Defense |
| CNSS | Committee on National Security Systems |
| Core 2 Year KU | 2-Year Institution – Core 2 Year 11 Mandatory KUs |
| Core 4-Year KU | 4-Year Institution – Core 4-Year 6 Mandatory KUs PLUS Core 2-year KUs |
| CWF  DCWS  DHS | Cybersecurity Workforce Framework  DoD Cyberspace Workforce Strategy  Department of Homeland Security |
| DoDD 8140 | Department of Defense Directive (DoDD) 8140, Cyberspace Workforce Management Policy Update |
| DoDD 8570 | Department of Defense Directive (DoDD) 8570, Workforce Improvement Program |
| Focus Area | Specialized areas providing valuable differentiation among institutions for marketing purpose |
| IA | Information Assurance |
| IACE | Information Assurance Curriculum Evaluation |
| KU | Knowledge Units are targeted technology areas composed of topics and expected outcomes; level-specific for 2-year, 4-year and graduate-level institutions; component of CAE Mapping Requirements |
| NICCS | National Initiative for Cybersecurity Careers and Studies |
| NICE | National Initiative for Cybersecurity Education |
| NICE Framework | National Cybersecurity Workforce Framework **provides a taxonomy and common lexicon to organize cybersecurity work** and workers |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| Optional KU | A set of 51 optional knowledge units from which 4-year CAEs must select and map to a minimum of five (5) |
| Specialty Area | Represents an area of concentrated work, or function, within the NIE Framework; 31 Specialty Areas |