NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

How to use the National Cybersecurity Workforce Framework

Your Implementation Guide

Margaret "Peggy" Maxson
Director, National Cybersecurity Education Strategy

A National Problem

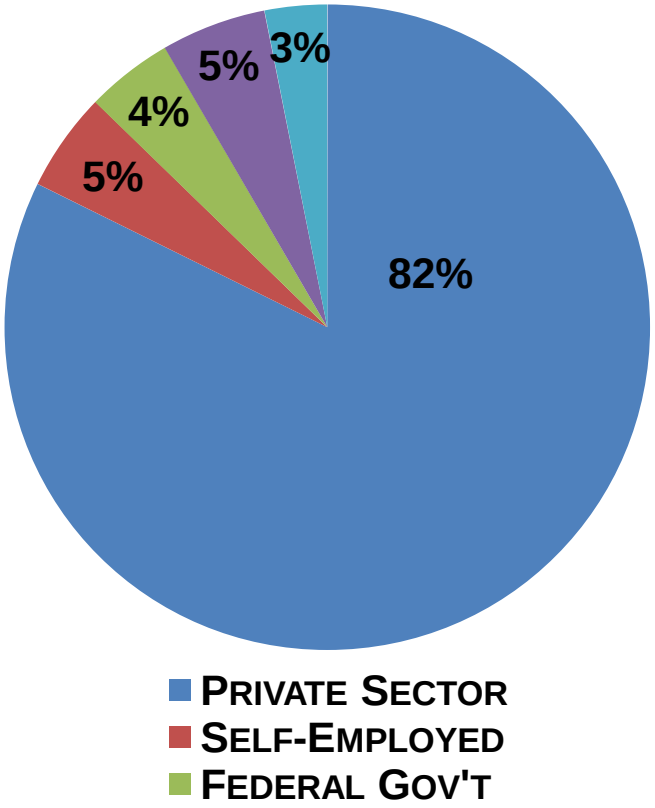
- The Nation needs greater cybersecurity awareness.
- The US workforce lacks cybersecurity experts.
- Many cybersecurity training programs exist but lack consistency among programs.
- Potential employees lack information about skills and abilities for cybersecurity jobs.
- Resources exist for teachers and students about cybersecurity but are difficult to find.
- Cybersecurity career development and scholarships are available but uncoordinated.
- Lack of communication between government, private industry, and academia.

The National Initiative for Cybersecurity Education (NICE) was established to raise national cybersecurity awareness, broaden the pool of cybersecurity workers through strong education programs, and build a globally competitive cybersecurity workforce.

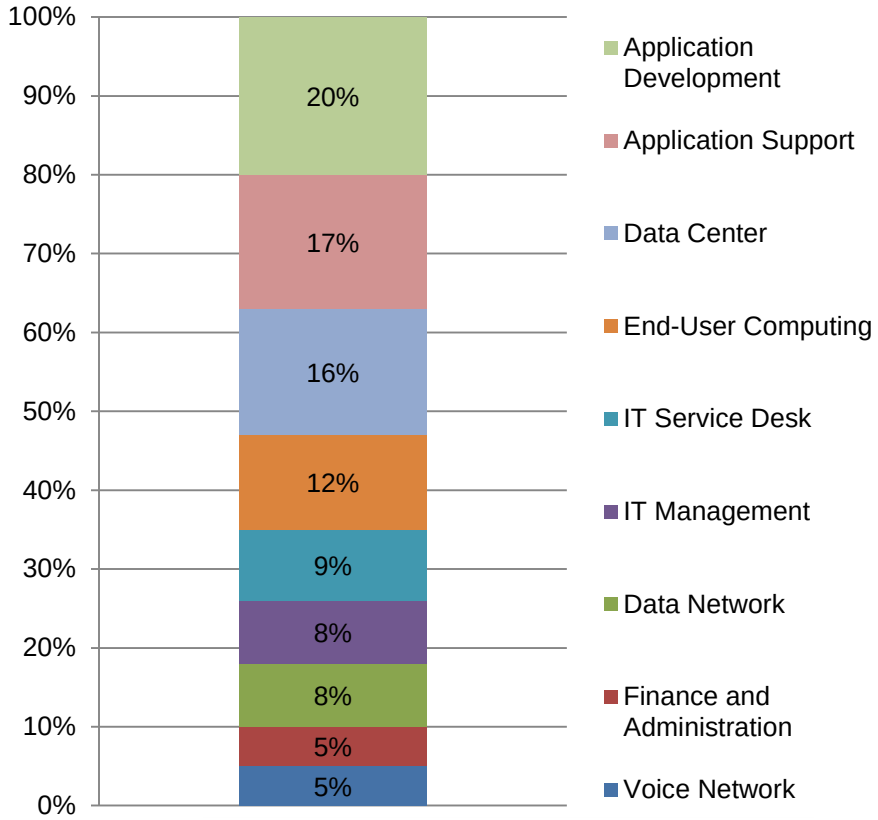
U.S. IT Workforce Statistics

According to the U.S. Bureau of Labor Statistics, there are approximately 4.0 million people employed in the U.S. IT labor workforce.

Percentage of IT Workers by Sector



Percentage of IT Workers by Technology Domain



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

*Source: CompTIA Colloquium 2012 - U.S. IT Market Supply and Demand Briefing

A SOLUTION

NICE developed the National Cybersecurity Workforce Framework (the Framework) to codify cybersecurity work and to identify the specialty areas of cybersecurity professionals.

The Framework establishes:

- A common taxonomy and lexicon for cybersecurity workers that organizes cybersecurity into 31 specialty areas within 7 categories.
- A baseline of tasks, specialty areas, and knowledge, skills and abilities (KSAs) associated with cybersecurity professionals.

The Framework assists with strategic human capital efforts, including:

- Workforce planning
- Recruitment and Selection
- Training and Development
- Succession Planning

CYBERSECURITY WORKFORCE FRAMEWORK

Work Plan Updates

Framework: A common language to define cybersecurity work. The Framework defines specialty areas, KSAs, and competencies.

- *Key Activities*: Version 1.0 Released (Aug 2012), LRM Process (Dec 2012 – Mar 2013), OPM Data Element Guidance (Oct 2012), Framework How-To Implementation Guide (Dec 2012), Framework Roll-out (Ongoing)*

Training Catalog / NICCS: An online web resource with a robust collection of trainings mapped to the Framework.

- *Key Activities*: Launch of the NICCS Portal (Dec 2012), Launch of the Training Catalog (Mar 2013)*

IT Workforce Assessment: Collect data to identify the current state of the information technology workforce, and to assess current cybersecurity capabilities.

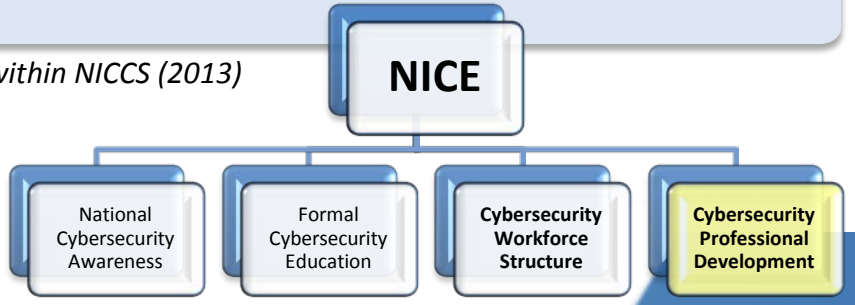
- *Key Activities*: Federal Pilot & Development (Oct 2012), Submit Federal Findings Report (Mar 2013)*

Training Gap Analysis: Ensure that available training is appropriate in terms of quality, need, and content.

- *Key Activities*: Workforce Current Training Needs Report (Mar 2013), Training Gap Analysis Report (Jun 2013)*

Professional Development Roadmaps: Develop resources which depict progression from entry to expert within each specialty area.

- *Key Activities*: Develop and Publish Professional Development Roadmaps within NICCS (2013)*



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

*Dates are subject to change based on availability of funding and resources.

Work Plan Updates

Centers for Academic Excellence (CAE) Knowledge Units (KUs): The Framework informed the development of the knowledge units.

- *Key Activities*: The KUs are in final development.*

Competition and Cyber Camp Mapping: Developing an inventory of cybersecurity competitions and cyber camps aligned to the specialty areas within the Framework.

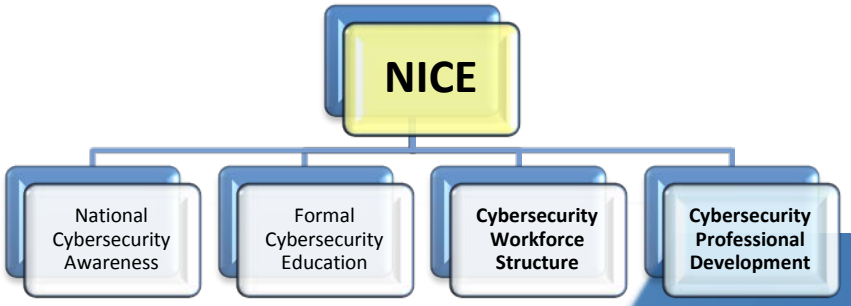
- *Key Activities*: Develop inventory of competitions and cyber camps (Ongoing), Post to NICCS Website (2013)*

Professionalization Seminars: Evaluate the merits of professionalizing the cybersecurity workforce. The National Academy of Science has been commissioned to hold public workshops across the country to gain insights in these efforts.

- *Key Dates*: Washington, D.C. (Dec 2012), San Francisco, CA (Feb 2013), San Antonio, TX (Mar 2013)*

Certification Mapping: Gather a listing of certifications and align each to the Framework. Make this information available on the NICCS website.

- *Key Activities*: Develop an inventory of certifications (Ongoing), Post to NICCS Website (2013)*



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

*Dates are subject to change based on availability of funding and resources.

THE FRAMEWORK IMPLEMENTATION HOW-TO GUIDE

To assist organizations with interpreting the Framework, NICE developed an interactive Implementation How-To Guide with instructions on how organizations can adopt the Framework to maintain consistency with this national standard.

The How-To Guide provides information on:

- Framework characteristics and the benefits of its use, and
- The importance of adopting the Framework.
- Human capital activities that are influenced by the Framework.
- Specific steps to apply the Framework to human capital activities.
- Cybersecurity roles, built by the Federal Chief Information Officer's Council. These roles are based on the Framework.
- Examples of how to define the workforce by using these specialty areas.
- A sample process to customize work roles based on the unique needs of an organization.

The benefits of the How-To Guide include:

- Helping streamline human capital efforts and fulfill the requirements of federal mandates.
- Detailing the Human Capital Lifecycle and how the framework will impact its development.
- Describing the OPM Data Element and how it will assist the organization and analysis of the cybersecurity workforce.
- Interactive functionality which simplifies navigating the guide.

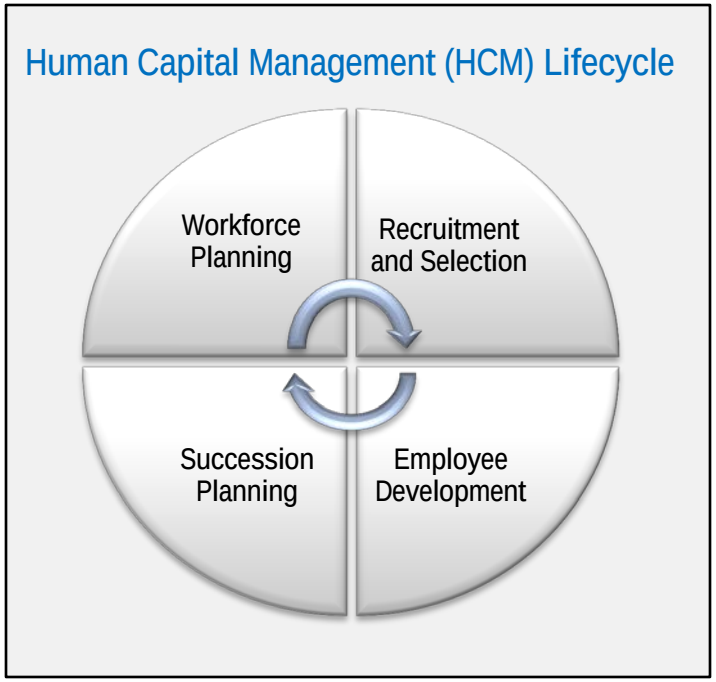
The interactive Implementation How-To Guide can be found on the NIST website: http://csrc.nist.gov/nice/framework/

Strategic Human Capital Planning

The Framework impacts every aspect of the Human Capital Management (HCM) Lifecycle. By using the How-To Guide, an agency can follow examples of how to incorporate the Framework into human capital activities.

The Framework does the following:

- Provides consistent language, role definitions, and a working taxonomy.
- Allows organizations to describe and define their cybersecurity workforces.
- Supports skill assessments and gap identification that can identify training needs of the workforce.
- Classifies workers into common cybersecurity roles.
- Promotes understanding of the work required of cybersecurity professionals.
- Redefines recruitment and selection procedures.
- Assists organizations with planning for future workforce needs.



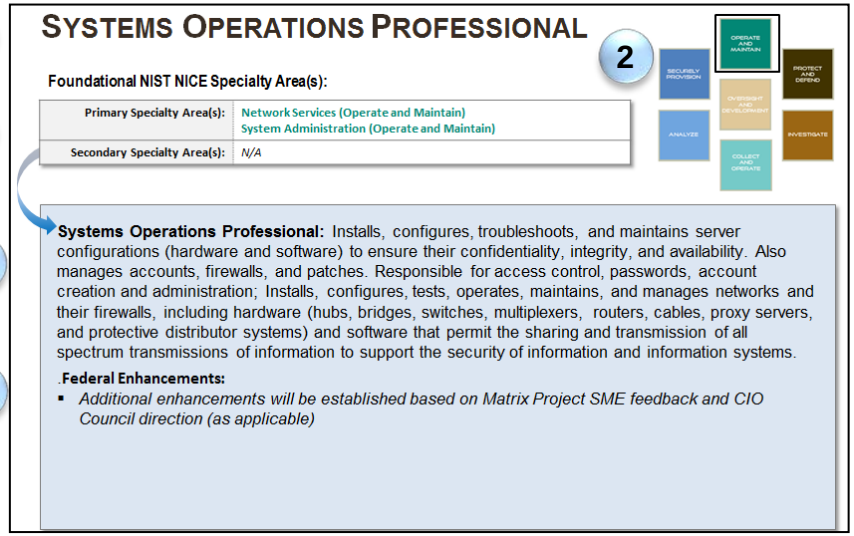
STREAMLINED ROLES (EXAMPLE)

If your organization has a limited number, or type, of cybersecurity positions, you may prefer to use the streamlined roles. The Federal Chief Information Officers Council (CIOC) developed 13 Framework-based roles to promote consistency and standardization of the cybersecurity workforce.

Each role consists of sample job titles and definition, the related Framework category, the Framework specialty areas, and any enhancements that pertain specifically to the Federal workforce.

1. Role Name
2. Framework Category
3. Framework Specialty Area
4. Sample Job Tasks
5. Federal Enhancements, if any

Streamlined Cybersecurity Role Example



The streamlined cyber roles developed by Fed CIOC:

- Systems Operations Professional
- Data Administrator
- Computer Network Defense (CND) Specialist
- Digital Forensics and Incident Response Analyst
- Information Security Auditor
- Information Systems Security Officer
- Information Systems Security Manager
- Information Security Architect
- Risk and Vulnerability Analyst
- Software Developer
- Information Systems Security Engineer
- Strategic Planning and Policy Development Professional
- Chief Information Security Officer (CISO)

CUSTOMIZED ROLE DEVELOPMENT

If your organization has many unique or specialized positions, you may choose to develop customized cybersecurity roles. This application has been demonstrated by DHS's Cyber Workforce Initiative (CWI).

An extensive review of DHS's workforce revealed many initial unique cybersecurity roles across the organization. DHS employed a process to establish generalized cybersecurity draft role categories linked to Fed CIOC Streamlined Roles, Framework Specialty Areas, Critical Skills, and the DHS Workforce.

DHS analyzed the following:

- Fed CIOC Streamlined Roles
- \+
- DHS Cybersecurity Professionals
- \+
- DHS HSAC CyberSkills Task Force

Customization

An analysis of the inputs on the left enabled DHS to develop the set of draft cybersecurity role categories on the right. The analysis included interviewing and other qualitative analysis activities.

23 ROLE CATEGORIES:

- **Chief Information Security Officer (CISO)/Chief Information Officer (CIO)**
- **Computer Network Defense (CND) Specialist**
- **Cyber Intelligence Operations & Analysis Professional**
- **Cyber Program/ Project Manager**
- **Cybersecurity Training, Outreach & Awareness Professional**
- **Cyber Workforce Planner**
- **Database Administrator (DBA)**
- **Forensic Examiner/Digital Media Analyst**
- **Incident Management & Incident Response (IMIR) Professional**
- **Information Security and Enterprise/ Systems Architect**
- **Information Security (INFOSEC) Auditor**
- **Information Systems Security Engineer (ISSE)**
- **Information Systems Security Manager (ISSM)**
- **Information Systems Security Officer (ISSO)**
- **Knowledge Officer**
- **Network Administrator**
- **Penetration Tester**
- **Risk & Vulnerability Specialist**
- **Secure Software Developer / Code Reviewer**
- **Standards and Research & Development Professional**
- **Strategic Planning & Policy Professional**
- **Systems Administrator**
- **Technical Customer Support**

Role Category Color LEGEND
RED - align to the 10 mission critical job tasks identified by the HSAC CyberSkills task Force.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

CUSTOMIZED ROLE (EXAMPLE)

Penetration Tester

Aligned DHS Roles to-date	**Vulnerability Assessment Programs (Blue Team)** **Penetration Tester (Red Team)** **Exploit Engineer/Developer**	
Prominent Specialty Areas: & Critical Task	• Systems Security Architecture • Security Engineering • Architecting for Building Security In • Information Assurance (IA) Compliance • Exploitation Analysis	• Application Penetration Tester • Vulnerability Assessment and Management • Systems Security Analysis • System and Network Penetration Tester • Penetration Testing

Role Definition: Follows a systematic methodology to assess, identify and demonstrate attack vectors and their impacts to provide risk mitigation/remediation strategies. Maintains knowledge of system architecture designs, current threats and methodologies (TTPs) and security requirements (e.g., NIST, FISMA, etc.) to conduct sophisticated penetration testing throughout the lifecycle. Demonstrates capability in running advanced exploitation techniques without the use of automated tools.

NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

***Source Definition:** Focus Group SMEs for System/Network/Application Penetration Testing

The National Initiative for Cybersecurity Careers and Studies (NICCS) Portal

Serves as the Nation's online resource for cybersecurity awareness, education, careers, training, and professional development.

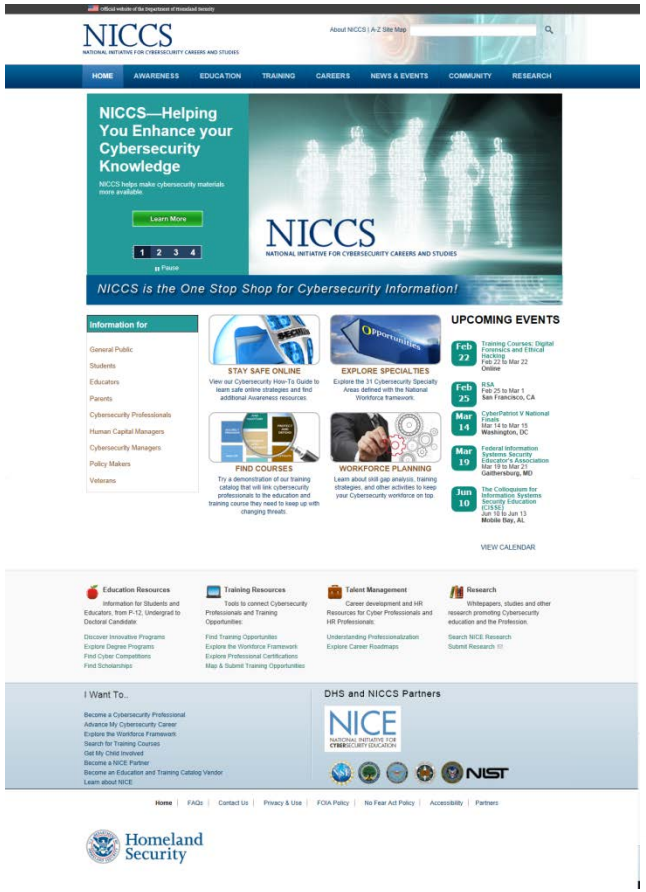
www.niccs.us-cert.gov

All inquiries: DHS Supervisory Office: niccs@hq.dhs.gov

Demonstration of NICCS!

Thursday, March 21st Portrait Room

10:30-1:30pm.



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NAVIGATING THE HOME PAGE

*The layout of the **Home Page** is designed to increase the visibility of NICE initiatives in an intuitive-format for the user.*

The banner at the top displays various links throughout the site.

The main page includes information for various demographic groups, such as students, professionals and veterans.

NAVIGATING THE TRAINING PAGE

*To access the Training Catalog, click on the **Training** tab.*

*On the training landing page, you can click either "**Training Catalog**," or the "**Find Courses**" button to enter the catalog.*

*Other links on this page will allow you to learn more about **the National Cybersecurity Workforce Framework**.*

NAVIGATING TRAINING: EXPLORE THE FRAMEWORK

The Training tab will also allow users to explore the National Cybersecurity Workforce Framework.

To explore the Framework, click the tab to the right of the Catalog Search tab, ***Explore the Framework****.*

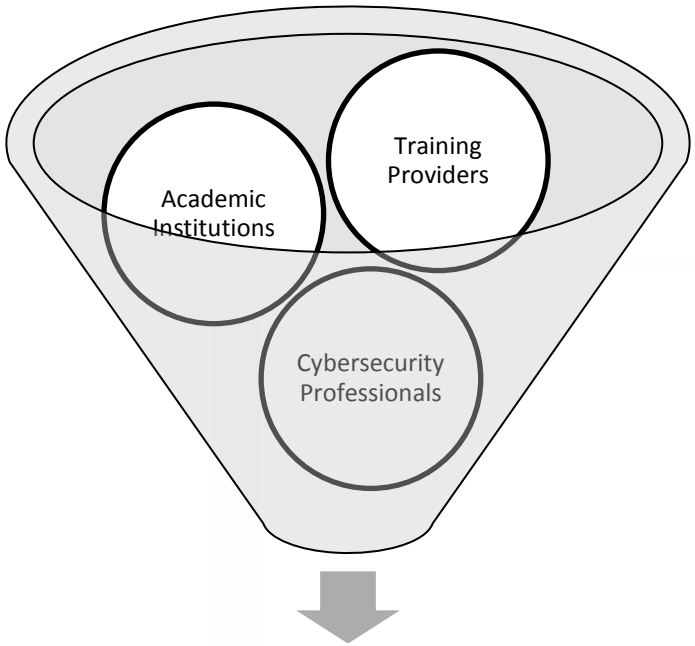
You can explore the Framework by clicking on ***Overview****,* ***Categories****,* ***Specialty Areas, KSAs****,* ***Competencies****, and* ***Tasks****.*

CYBERSECURITY TRAINING AND EDUCATION CATALOG

To promote cybersecurity education, and to provide a comprehensive resource for the Nation, NICE developed the Cybersecurity Training and Education Catalog. The Cybersecurity Training and Education Catalog will be hosted on the NICCS Portal.

Benefits of of the Cybersecurity Training and Education Catalog include the following:

- Brings together cybersecurity professionals, training providers, and academic institutions in an interactive online environment.
- Provides a repository of cybersecurity knowledge and a one stop shop for all types of cybersecurity training.
- Allows the general public to easily and quickly access cybersecurity training suited to their needs.



NAVIGATING THE CATALOG: TRAINING SEARCH

*To search the Training Catalog, click on the **Catalog Search** Tab.*

*Cyber Professionals can use the Training Catalog to search available courses by **Specialty Area**, **Keyword**, **Provider**.*

*Training can also be browsed using the interactive Framework Specialty Areas by clicking **Browse Courses using the Workforce Framework**.*

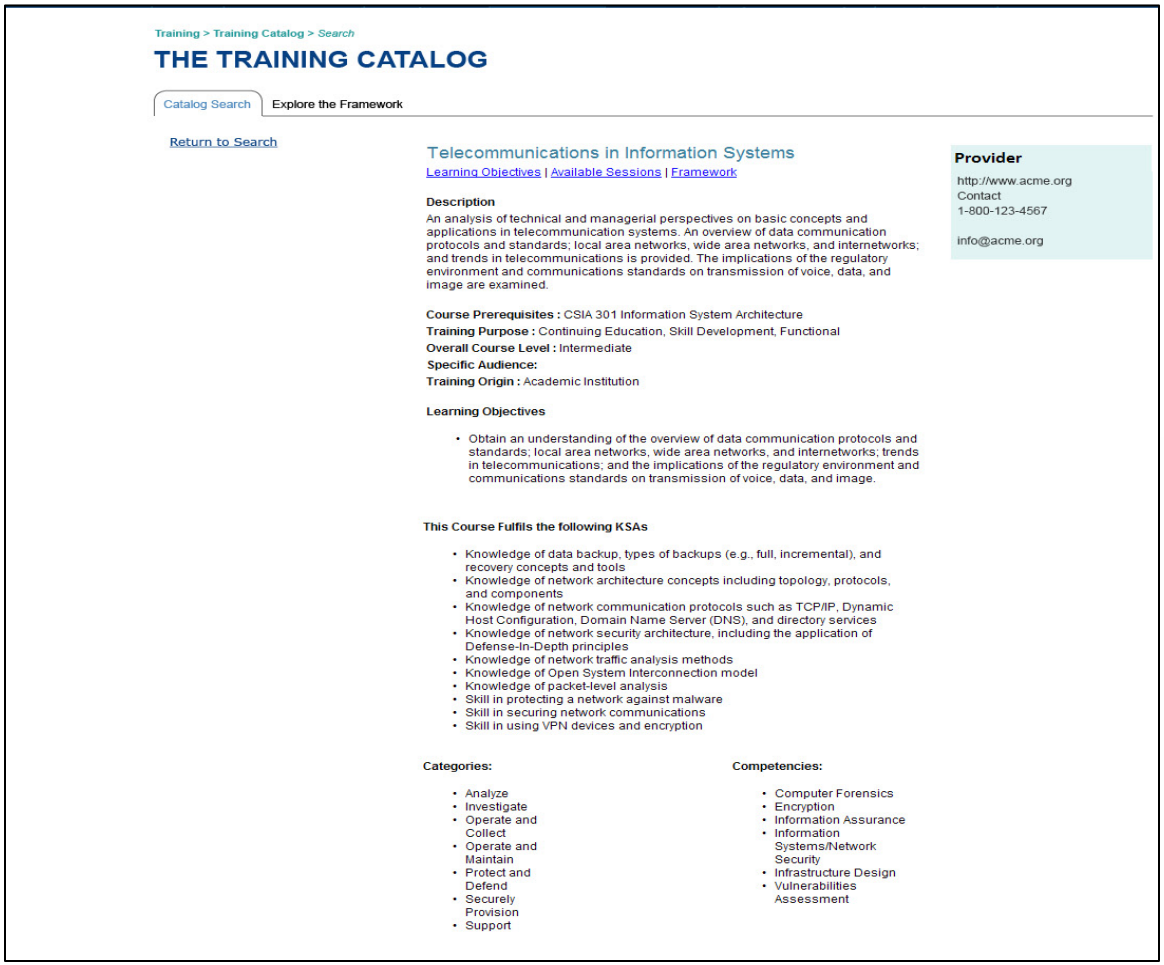
NAVIGATING THE CATALOG: EXPLORE THE FRAMEWORK SPECIALTY AREAS

Initially, the Cybersecurity Training and Education Catalog training is mapped to the Framework Specialty Areas. In future phases of the Cybersecurity Training and Education Catalog, courses may also be mapped to Knowledge, Skills, and Abilities.

You can explore the Workforce Specialty Areas by clicking the tab ***Specialty Area.***

Each specialty area page includes a description, related job titles, a list of sample tasks, and examples of KSAs.

Navigating the Catalog: Training Course Description



Training > Training Catalog > *Search*

THE TRAINING CATALOG

Catalog Search | Explore the Framework

Return to Search

Telecommunications in Information Systems

Learning Objectives | Available Sessions | Framework

Provider

http://www.acme.org
Contact
1-800-123-4567

info@acme.org

Description

An analysis of technical and managerial perspectives on basic concepts and applications in telecommunication systems. An overview of data communication protocols and standards; local area networks, wide area networks, and internetworks; and trends in telecommunications is provided. The implications of the regulatory environment and communications standards on transmission of voice, data, and image are examined.

Course Prerequisites : CSIA 301 Information System Architecture
Training Purpose : Continuing Education, Skill Development, Functional
Overall Course Level : Intermediate
Specific Audience:
Training Origin : Academic Institution

Learning Objectives

- Obtain an understanding of the overview of data communication protocols and standards; local area networks, wide area networks, and internetworks; trends in telecommunications; and the implications of the regulatory environment and communications standards on transmission of voice, data, and image.

This Course Fulfils the following KSAs

- Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools
- Knowledge of network architecture concepts including topology, protocols, and components
- Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services
- Knowledge of network security architecture, including the application of Defense-In-Depth principles
- Knowledge of network traffic analysis methods
- Knowledge of Open System Interconnection model
- Knowledge of packet-level analysis
- Skill in protecting a network against malware
- Skill in securing network communications
- Skill in using VPN devices and encryption

Categories:

- Analyze
- Investigate
- Operate and Collect
- Operate and Maintain
- Protect and Defend
- Securely Provision
- Support

Competencies:

- Computer Forensics
- Encryption
- Information Assurance
- Information Systems/Network Security
- Infrastructure Design
- Vulnerabilities Assessment

The Training information page provides the following information:

- ***Description***
- ***Provider***
- ***Course Prerequisites***
- ***Training Purpose***
- ***Overall Course Level***
- ***Audience***
- ***Training Origin***
- ***Learning Objectives***
- ***Framework Categories and Competencies***

Aligning Courses to Specialty Areas: Proficiency Level Descriptions

When you complete the Cybersecurity Training Data Collection Form, you will be asked to select the training proficiency level for each course. This information will assist individuals in selecting the appropriate level of required training. The proficiency levels are defined below:

Level	Description
0	This training is intended for someone with insufficient knowledge, skill, or ability level necessary for use in simple or routine work situations. Knowledge, skill, or ability level provided would be similar to the knowledge of a layperson. Considered “no proficiency” for purposes of accomplishing specialized, or technical, work.
1	This training is intended for individuals who need **basic knowledge, skills, or abilities** necessary for use and the application in simple work situations with specific instructions and/or guidance.
2	This training is intended for individuals who need **intermediate knowledge, skills, or abilities** for independent use and application in straightforward, routine work situations with limited need for direction.
3	This training is intended for individuals who need **advanced knowledge, skills, or abilities** for independent use and application in complex or novel work situations.
4	This training is intended for individuals who need **expert knowledge, skills, or abilities** for independent use and application in highly complex, difficult, or ambiguous work situations, or the trainee is an acknowledged authority, advisor, or key resource.

How will the Information be Monitored?

The NICCS Portal, and the Cybersecurity Training and Education Catalog, are monitored by the NICCS Supervisory Office (SO). The SO is responsible for the following:

- Responding to emails to the NICCS SO general mailbox.
- Reviewing the website daily to fix any errors or to edit inaccurate information.
- Updating the site with timely information and additional cybersecurity training and education information.
- Partnering with cybersecurity training providers to help post training to the Cybersecurity Training and Education Catalog.
- If you notice any that needs to be fixed on the website, please let us know! You can email us at NICCS@hq.dhs.gov.

Next Steps

Your assistance is critical to defining and creating a high-performing cybersecurity workforce. Next steps include:

- Exploring the NICCS website and learning how your organization can become involved.
- Becoming familiar with the Framework and its significance in human capital planning.
- Identifying points of contact (POCs) and champions in your organization to identify how to best adopt the Framework.
- Using the following How-To Guide to decide how to tailor the Framework to your organization's workforce needs.
- Establishing an internal plan for adopting the Framework.
- Communicating the Framework with your network of colleagues.
- Linking implementation of the Framework to the Closing the Skills Gap effort.
- Developing Framework Version 2.0 beginning on June 21st, 2013.

BACKUP SLIDES

White House Definition of Cybersecurity

Cybersecurity professionals are involved in activities that include "…strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. "

-Cyberspace Policy Review, May 2009

Framework Categories and Specialty Areas

*The Framework organizes cybersecurity work into 31 specialty areas within 7 categories. Each specialty area represents an area of concentrated work, or function, within cybersecurity. Below are the 7 categories (**bold**), with corresponding specialty areas.*

Securely Provision
- Systems Requirements Planning
- Systems Development
- Software Assurance and Security Engineering
- Systems Security Architecture
- Test and Evaluation
- Technology Research and Development
- Information Assurance (IA) Compliance

Operate and Maintain
- System Administration
- Network Services
- Systems Security Analysis
- Customer Service and Technical Support
- Data Administration
- Knowledge Management

Collect and Operate
- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Protect and Defend
- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense (CND) Analysis
- Computer Network Defense (CND) Infrastructure Support

Investigate
- Investigation
- Digital Forensics

Analyze
- Cyber Threat Analysis
- Exploitation Analysis
- Targets
- All Source Intelligence

Oversight and Development
- Legal Advice and Advocacy
- Education and Training
- Strategic Planning and Policy Development
- Information Systems Security Operations (ISSO)
- Security Program Management (Chief Information Security Officer [CISO])

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION