NICE

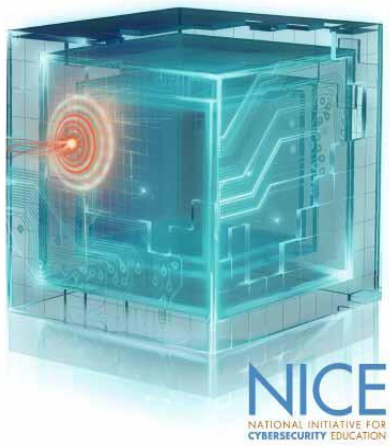
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Cybersecurity Workforce Framework Tutorial

Jane Homeyer, Ph.D., Deputy ADNI/HC for Skills and Human Capital Data, ODNI
Margaret Maxson, Director, National Cybersecurity Education Strategy, DHS

Outline for Today

- Introduction to NICE
- NICE Workforce Plan Overview
- Introduction to the Cybersecurity Workforce Framework
- Exercise 1: *Review of the Framework*
- Case Study: DHS Pilot Implementation
- Exercise 2: *Linking Training to the Framework*
- Call to Action



Introduction to NICE

- The National Initiative for Cyber Security Education (NICE) is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development.

- The mission of NICE is to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace for all.

NICE Component 4 – Workforce Training and Professional Development

- This component is responsible for:
  - defining the cybersecurity workforce; and
  - identifying the training and professional development required for the nation's cybersecurity workforce.

- Lead by the DoD, ODNI and DHS, in coordination with academia, industry and state, local and tribal governments.

Understanding the Cybersecurity Workforce

We need the answers to questions such as:

- Who is a cybersecurity professional?
- Do we know in our Federal Government employee population, who works in cybersecurity and what their capabilities are?
- How many cybersecurity professionals receive annual performance awards in comparison to professionals in other occupations?
- What is the average starting salary of an System Architect within various Federal Government organizations? How does this compare to private industry?
- What are the average promotion rates of different cybersecurity specialties compared to one another and to other occupations?
- What are the attrition rates?
- Etc….

NICE Workforce Plan Overview

Need for Standardization

- Today, there is very little consistency throughout the Federal Government and the Nation in terms of how cybersecurity work is defined, described, and how the workforce is trained.

- Establishing and implementing standards for cybersecurity workforce and training is a foundational component for every workforce plan.

Component 4 Work Plan – Task Overview

- Task 1 – Population Review – Defining the Workforce – The Framework
- Task 2 – Training Catalog – Identifying the Training Per Level
- Task 3 – Workforce Baseline Study – Assess the Quality
- Task 4 – Workforce & Training Analysis (Identification of gaps in capabilities and available training) – Identification of Gaps
- Task 5 – Professional Development Roadmaps – The Pipeline
- Task 6 - Communication

Federal Department and Agency Support

Over 20 Federal Departments and Agencies participated to develop the framework, including:

Department of State
Department of Education
Department of Labor
Office of Management and Budget
Office of Personnel Management
Department of Defense
Department of Justice
Information Sciences & Technologies
Department of Homeland Security (including NPPD, TSA, USSS, Coast Guard, ICE, CBP, CIS, DHS OI&A).

Central Intelligence Agency
Defense Intelligence Agency
Director of National Intelligence
Federal Bureau of Investigation
National Security Agency
National Science Foundation
Department of Defense /DC3x
National Counterintelligence Executive
Federal CIO Council

Non-Profit & Government Organizations

In addition, NICE has worked very closely with non-profit and governmental organizations to socialize the framework. Including, but not limited to:

- FedCIO Council IT Work Force Committee (ITWFC)
- Committee of National Systems Security (CNSS)
- FedCIO Council Information Security and Identity Management Committee (ISIMC)
- National Cybersecurity Alliance (NCSA)
- Federal Information Systems Security Educators Association (FISSEA)
- Colloquium for Information Systems Security Educators (CISSE)
- Colloquium for Advanced Cybersecurity Education (CACE)
- Washington Cyber Roundtable
- CyberWatch
- US Cyber Challenge
- National Association of State Chief Information Officers (NASCIO)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Information Systems Security Association (ISSA)
- National Board of Information security Examiners (NBISE)
- Cybersecurity Certification Collaborative (C3)
- Institute for Information Infrastructure Protection (I3P)
- Association for Computing machinery (ACM)
- Institute of Electrical and Electronics Engineers (IEEE)

Cybersecurity Workforce Framework

Framework Development Process

1

Conducting Internet searches and collecting documents (reports, websites, briefings, etc.) from across the government related to workforce constructs such as:

Computer network defense (CND) service provider organizations, Computer network operations (CNO), Cyber investigation, Cybersecurity , Counterintelligence, Counterintelligence in Cyberspace, IT infrastructure, operations, development and information assurance.

2

Sample reviewed documents included: Some of the reviewed documents were:

Office of Personnel Management's occupational standards (OPM, 2010), Job descriptions from the Department of Labor's O*NET database (2010), DoD 8570.01-M Information Assurance Workforce Improvement Program (DoD, 2010), DoD Cybersecurity Workforce Framework, DoD Counterintelligence in Cyberspace Training and Professional Development Plan, Federal Cybersecurity Workforce Transformation Working Group Report on Cybersecurity Competencies

3 Refine existing definitions of cybersecurity specialty areas based on collected information

4 Conduct focus groups with subject matter experts to identify and define specialty areas not noted in previous documents

5 New specialty areas included Investigation, Technology Demonstration, Information Systems Security Management, etc.

6 Review existing task and KSA statements that define the work within specialty areas.

7 Identify, collect, write new task and KSA statements where appropriate.

8 Gather SME input on task and KSA statements.

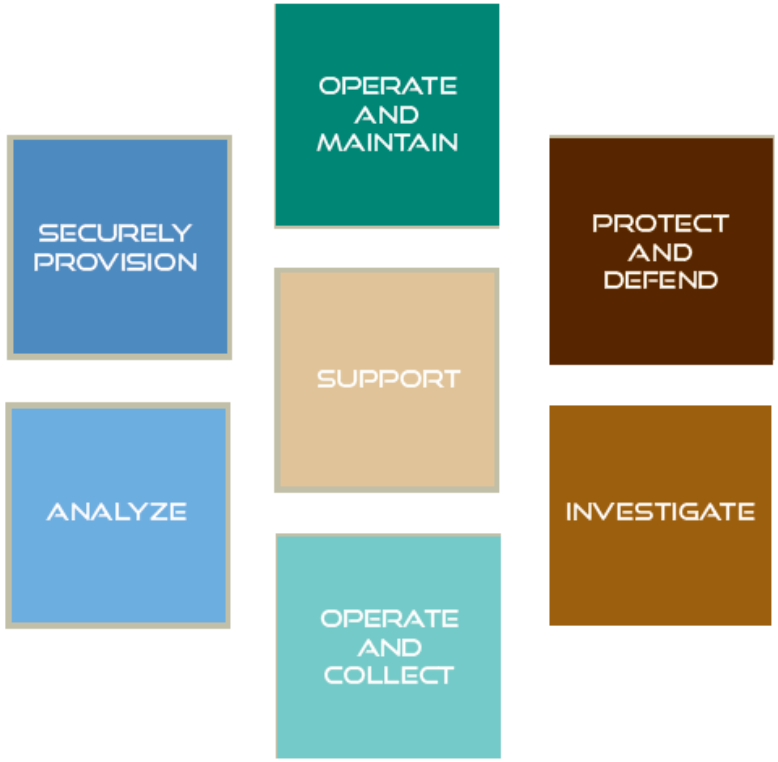
9 Refine framework as necessary through workshops, meetings, and stakeholder input.

ongoing

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Framework Categories

The **Framework** *organizes cybersecurity into **seven** high-level categories, each comprised of several specialty areas.*

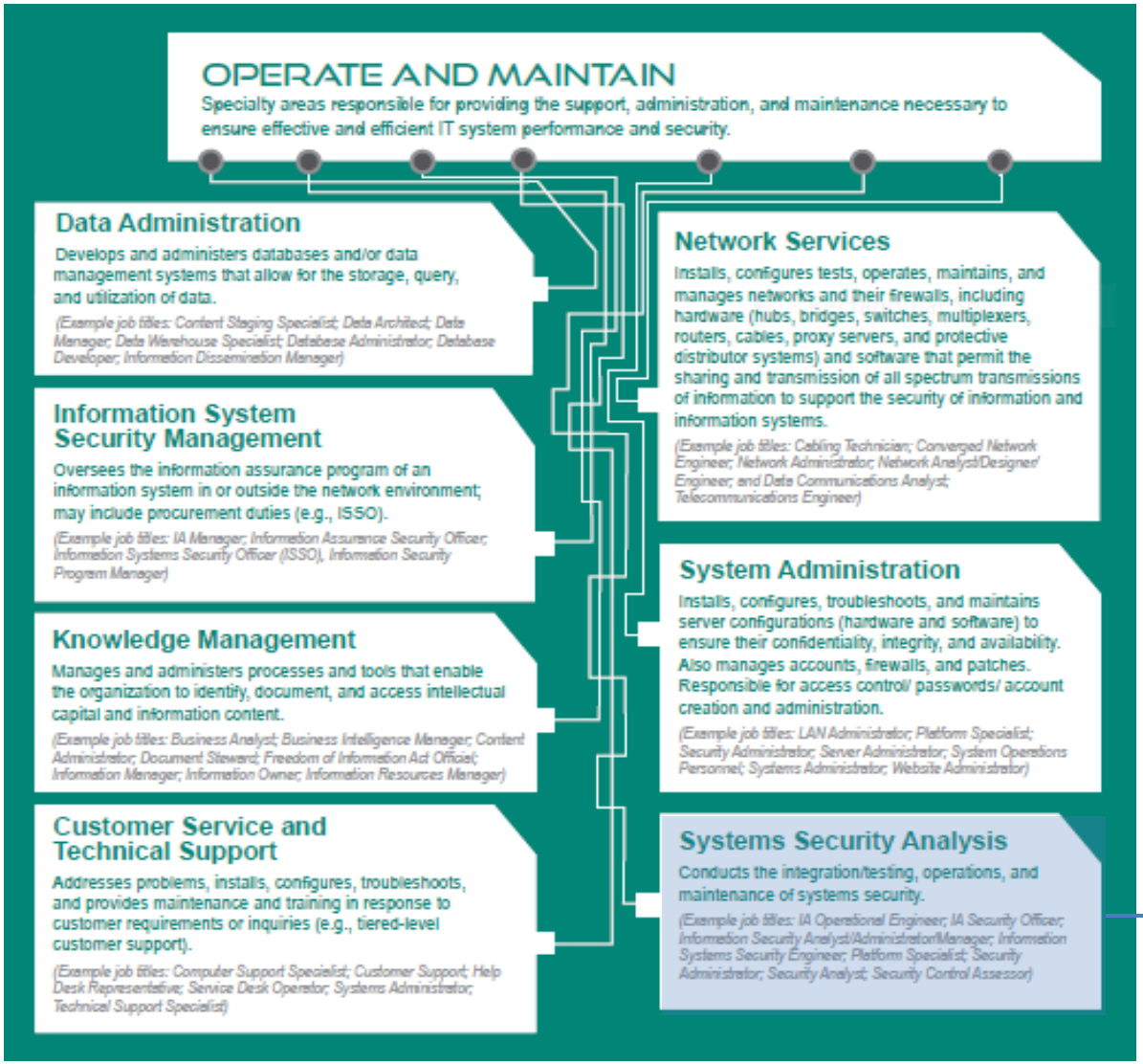


CYBERSECURITY WORKFORCE FRAMEWORK

7 Categories – Each Comprising Several Specialty Areas

Securely Provision	Specialty areas concerned with conceptualizing, designing, and building secure IT systems.
Operate and Maintain	Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Specialty area responsible for the identification, analysis and mitigation of threats to IT systems and networks.
Investigate	Specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Operate and Collect	Specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Specialty area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
Support	Specialty areas that provide critical support so that others may effectively conduct their cybersecurity work.

Example Category and its Specialty Areas



"So…What else do I get?"

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Category: Operate and Maintain	
Specialty Area: Systems Security Analysis	
Responsible for the integration/testing, operations and maintenance of systems security	
Typical OPM Classification: 2210, Information Technology Management *(Actual information provided by OPM)*	
Example Job Titles: Information Assurance Security Information System Security Information Systems Security IA Operational Engineer	
Job Tasks 1. Implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation. 2. Implement approaches to resolve vulnerabilities, mitigate risks and recommend security changes to system or system components as needed. 3. Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy. 4. Etc…..	
Competency	**KSA**
Information Assurance: Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality and integrity.	Skill in determining how a security system should work.
	Knowledge of security management
	Knowledge of Information Assurance principles and tenets.
Risk Management: Knowledge of the principles, methods, and tools used for risk assessment and mitigation, including assessment of failures and their consequences.	Knowledge of risk management processes, including steps and methods for assessing risk.
	Knowledge of network access and authorization (e.g. PKI)
	Skill in, assessing the robustness of security systems and designs.
System Life Cycle: Knowledge of systems life cycle management concepts used to plan, develop, implement, operate and maintain information systems.	Knowledge of system lifecycle management principals.
	Knowledge of how system components are installed, integrated and optimized.
	Skill in designing the integration of hardware and software solutions.

Exercise 1: Review of the Cybersecurity Workforce Framework

Overall Framework Review

General Overview

- ***What does the NICE Cybersecurity Workforce Framework cover?***
- ***What is a specialty area?***

Let's Begin Part 1:

- Take 5-10 minutes to independently review the "paint chip" booklet
  - Look at the overall structure of categories and the specialty areas within them
  - Read the definitions of the each specialty area and consider how well it fits into the category

Questions to Consider

- Can you identify a specialty area that describes your primary job responsibilities?
- Are the specialty areas appropriately grouped within each major category (i.e., Securely Provision, Operate and Maintain, Protect and Defend, etc.)?
- What specialty areas are missing?
- Should any specialty areas should be deleted?

Part 2 – Specialty Area Deep Dive Review

- Group 1 – Independent review of Tasks/KSAs
- Group 2 – Group discussion of Information Systems Security Management, Security Program Management, and Strategic Planning and Policy Development
- Group 3 – IT Program Management

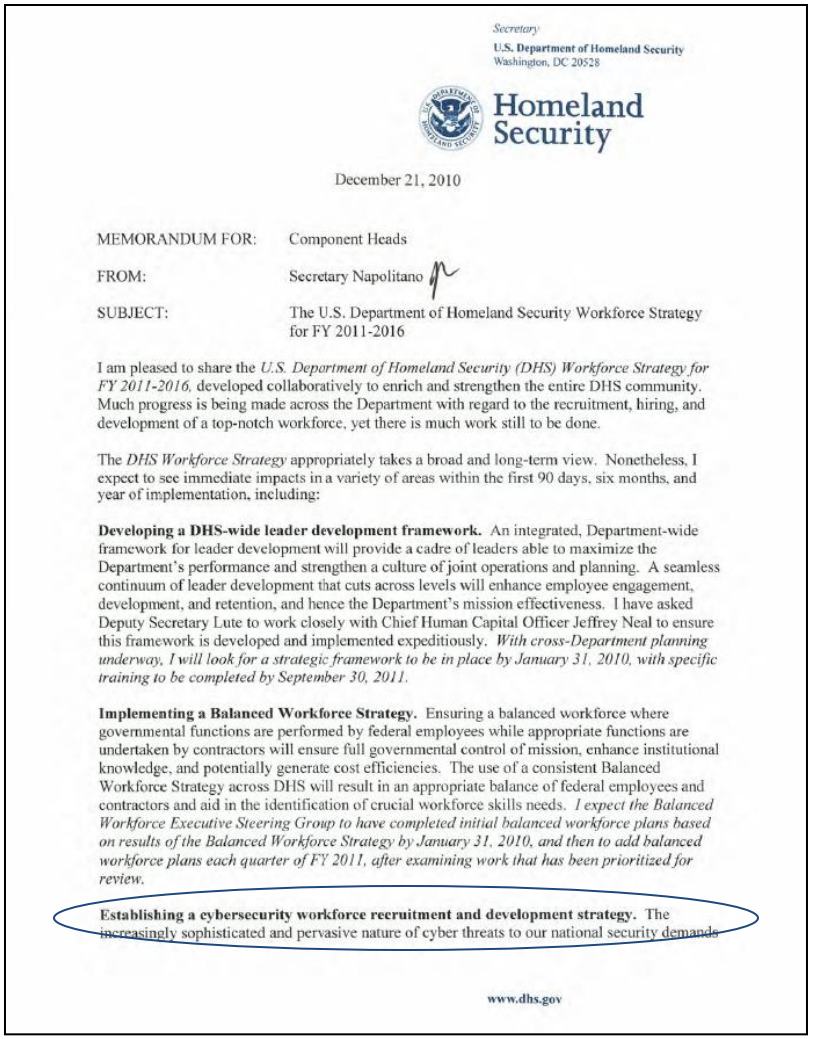
Small Group Facilitators will provide additional Guidance

Case Study:
DHS Pilot Implementation

DHS Cyber Workforce Initiative

The Secretary of the Department of Homeland Security has identified the acquiring, growing, and sustaining of a cyber workforce as one of the Department's priorities

- The cyber security mission of DHS will require a federal workforce that possesses the necessary skills to lead cybersecurity missions and solutions, while ensuring the future security of the national critical infrastructure
- In response, the Office of the Chief Human Capital Officer (OCHCO) and the National Protection and Programs Directorate (NPPD) has established a cross-component team responsible for the development of this initiative



Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

December 21, 2010

MEMORANDUM FOR: Component Heads

FROM: Secretary Napolitano

SUBJECT: The U.S. Department of Homeland Security Workforce Strategy for FY 2011-2016

I am pleased to share the *U.S. Department of Homeland Security (DHS) Workforce Strategy for FY 2011-2016*, developed collaboratively to enrich and strengthen the entire DHS community. Much progress is being made across the Department with regard to the recruitment, hiring, and development of a top-notch workforce, yet there is much work still to be done.

The *DHS Workforce Strategy* appropriately takes a broad and long-term view. Nonetheless, I expect to see immediate impacts in a variety of areas within the first 90 days, six months, and year of implementation, including:

Developing a DHS-wide leader development framework. An integrated, Department-wide framework for leader development will provide a cadre of leaders able to maximize the Department's performance and strengthen a culture of joint operations and planning. A seamless continuum of leader development that cuts across levels will enhance employee engagement, development, and retention, and hence the Department's mission effectiveness. I have asked Deputy Secretary Lute to work closely with Chief Human Capital Officer Jeffrey Neal to ensure this framework is developed and implemented expeditiously. *With cross-Department planning underway, I will look for a strategic framework to be in place by January 31, 2010, with specific training to be completed by September 30, 2011.*

Implementing a Balanced Workforce Strategy. Ensuring a balanced workforce where governmental functions are performed by federal employees while appropriate functions are undertaken by contractors will ensure full governmental control of mission, enhance institutional knowledge, and potentially generate cost efficiencies. The use of a consistent Balanced Workforce Strategy across DHS will result in an appropriate balance of federal employees and contractors and aid in the identification of crucial workforce skills needs. *I expect the Balanced Workforce Executive Steering Group to have completed initial balanced workforce plans based on results of the Balanced Workforce Strategy by January 31, 2010, and then to add balanced workforce plans each quarter of FY 2011, after examining work that has been prioritized for review.*

Establishing a cybersecurity workforce recruitment and development strategy. The increasingly sophisticated and pervasive nature of cyber threats to our national security demands

www.dhs.gov

"Eating a Pack of Elephants"

With all the organizational considerations in building and sustaining a Cyber Workforce for DHS, where should we start?

- Strategic Plan – 4 Major Goals
  - Identify parameters for building an effective, mission-focused cybersecurity workforce;
  - Recruit highly qualified cybersecurity workforce professionals and leaders;
  - Grow individual and organizational capabilities to promote a highly-qualified workforce; and
  - Sustain an engaged cybersecurity workforce and leadership cadre by sharing institutional knowledge and promoting a unified DHS culture
- Implementation

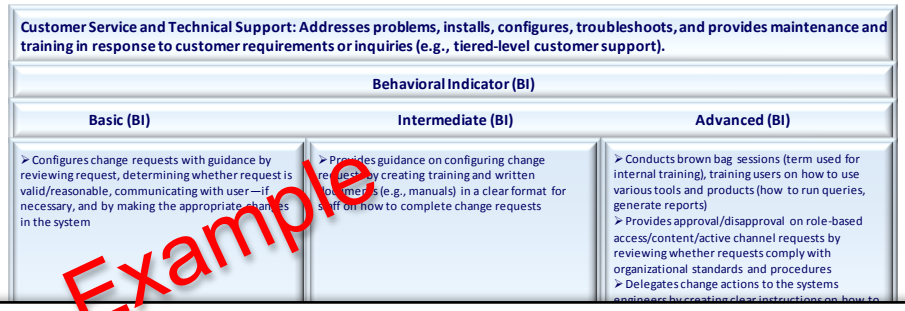
Implementation: First Steps

To start, Cyber Workforce Development is focused on defining C*apability* needs, which is accomplished by building competency models

- Why Cyber Competency Models?
  - Objective: Competencies define the skills/capabilities critical for successful job performance across Cyber roles, and the behaviors that exemplify the progressive levels of proficiency associated with these competencies
  - Impact: Provides a solid foundation upon which targeted recruitment, selection, and employee development (learning and training) initiatives can be built to increase Cyber Workforce capabilities

What makes a Competency Model?

- Competencies
- Behavioral Indicators



Competency	Definition
Penetration Testing	Designs, simulates, and executes attacks on networks and systems. Leverages existing and emerging methods to attack systems and exploit vulnerabilities. Documents penetration testing methodology, findings, and resulting business impact.

Implementation: Challenges

- How do we minimize the time impact on the managers, supervisors and SMEs?
- How do we ensure consistency in terminology across all agencies and components?
- Who are the DHS Cybersecurity professionals?
- What competency work has been accomplished?
- With so many Occupational Series involved with Cybersecurity, how should the models be built?

A NICE Solution

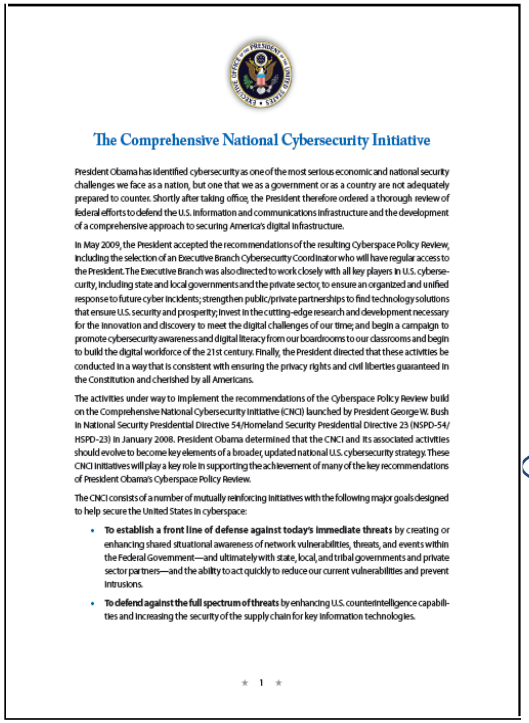
Although we still have some outstanding challenges, the NICE Framework presented an exceptional solution for time and consistency. Using the framework as a foundation, DHS can

- Compile initial technical competency models in a compressed timeframe
- Maintain consistency in terminology across all agencies and components, as well as alignment with NICE and OPM

Rollout Experience: The story we had to tell

People need/want to know where the Framework came from and why it was developed

The Comprehensive National Cybersecurity Initiative – Initiative #8 – requires building a national Cyber Workforce and serves as the foundation for the National Initiative Cybersecurity Education (NICE)



The Comprehensive National Cybersecurity Initiative

President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter. Shortly after taking office, the President therefore ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing America's digital infrastructure.

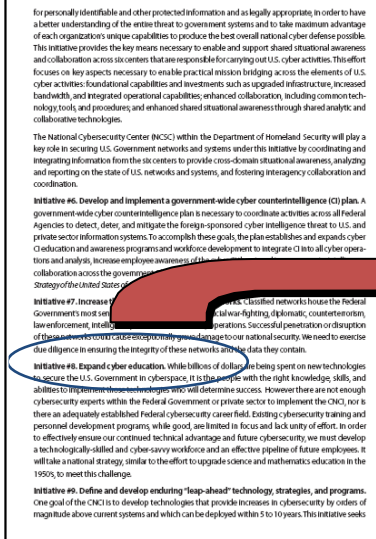
In May 2009, the President accepted the recommendations of the resulting Cyberspace Policy Review, including the selection of an Executive Branch Cybersecurity Coordinator who will have regular access to the President. The Executive Branch was also directed to work closely with all key players in U.S. cybersecurity, including state and local governments and the private sector, to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure U.S. security and prosperity; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; and begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century. Finally, the President directed that these activities be conducted in a way that is consistent with ensuring the privacy rights and civil liberties guaranteed in the Constitution and cherished by all Americans.

The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. These CNCI initiatives will play a key role in supporting the achievement of many of the key recommendations of President Obama's Cyberspace Policy Review.

The CNCI consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

- **To establish a front line of defense against today's immediate threats** by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
- **To defend against the full spectrum of threats** by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.

* 1 *



for personally identifiable and other protected information and as legally appropriate, in order to have a better understanding of the entire threat to government systems and to take maximum advantage of each organization's unique capabilities to produce the best overall national cyber defense possible. This initiative provides the key means necessary to enable and support shared situational awareness and collaboration across six centers that are responsible for carrying out U.S. cyber activities. This effort focuses on key aspects necessary to enable practical mission bridging across the elements of U.S. cyber activities: foundational capabilities and investments such as upgraded infrastructure, increased bandwidth, and integrated operational capabilities; enhanced collaboration, including common technology, tools, and procedures; and enhanced shared situational awareness through shared analytic and collaborative technologies.

The National Cybersecurity Center (NCSC) within the Department of Homeland Security will play a key role in securing U.S. Government networks and systems under this initiative by coordinating and integrating information from the six centers to provide cross-domain situational awareness, analyzing and reporting on the state of U.S. networks and systems, and fostering interagency collaboration and coordination.

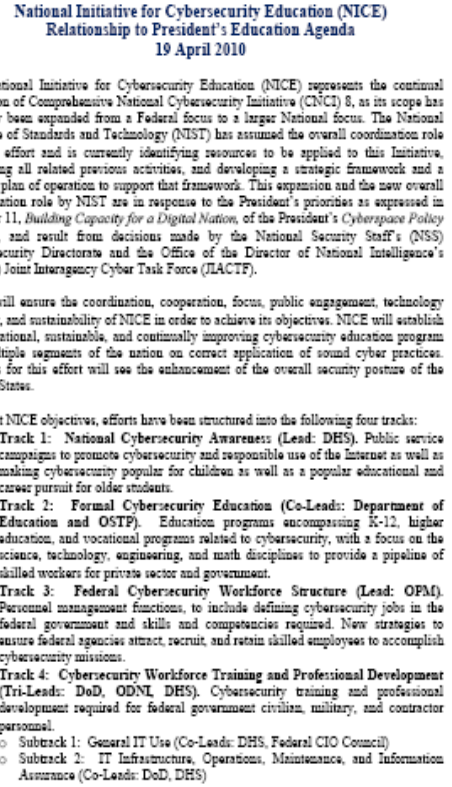
Initiative #6. Develop and implement a government-wide cyber counterintelligence (CI) plan. A government-wide cyber counterintelligence plan is necessary to coordinate activities across all Federal Agencies to detect, deter, and mitigate the foreign-sponsored cyber intelligence threat to U.S. and private sector information systems. To accomplish these goals, the plan establishes and expands cyber CI education and awareness programs and workforce development to integrate CI into all cyber operations and analysis, increase employee awareness of the [illegible] collaboration across the government [illegible] *Strategy of the United States of*

Initiative #7. Increase [illegible] U.S. classified networks house the Federal Government's most sen[illegible] cal war-fighting, diplomatic, counterterrorism, law enforcement, intelli[illegible] operations. Successful penetration or disruption of these networks could exceptionally grave damage to our national security. We need to exercise due diligence in ensuring the integrity of these networks and the data they contain.

Initiative #8. Expand cyber education. While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement these technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge.

Initiative #9. Define and develop enduring "leap-ahead" technology, strategies, and programs. One goal of the CNCI is to develop technologies that provide increases in cybersecurity by orders of magnitude above current systems and which can be deployed within 5 to 10 years. This initiative seeks

* 4 *



National Initiative for Cybersecurity Education (NICE)
Relationship to President's Education Agenda
19 April 2010

The National Initiative for Cybersecurity Education (NICE) represents the continual evolution of Comprehensive National Cybersecurity Initiative (CNCI) 8, as its scope has recently been expanded from a Federal focus to a larger National focus. The National Institute of Standards and Technology (NIST) has assumed the overall coordination role for the effort and is currently identifying resources to be applied to this Initiative, reviewing all related previous activities, and developing a strategic framework and a tactical plan of operation to support that framework. This expansion and the new overall coordination role by NIST are in response to the President's priorities as expressed in Chapter 11, *Building Capacity for a Digital Nation*, of the President's *Cyberspace Policy Review*, and result from decisions made by the National Security Staff's (NSS) Cybersecurity Directorate and the Office of the Director of National Intelligence's (ODNI) Joint Interagency Cyber Task Force (JIACTF).

NIST will ensure the coordination, cooperation, focus, public engagement, technology transfer, and sustainability of NICE in order to achieve its objectives. NICE will establish an operational, sustainable, and continually improving cybersecurity education program for multiple segments of the nation on correct application of sound cyber practices. Success for this effort will see the enhancement of the overall security posture of the United States.

To meet NICE objectives, efforts have been structured into the following four tracks:

- **Track 1: National Cybersecurity Awareness (Lead: DHS).** Public service campaigns to promote cybersecurity and responsible use of the Internet as well as making cybersecurity popular for children as well as a popular educational and career pursuit for older students.
- **Track 2: Formal Cybersecurity Education (Co-Leads: Department of Education and OSTP).** Education programs encompassing K-12, higher education, and vocational programs related to cybersecurity, with a focus on the science, technology, engineering, and math disciplines to provide a pipeline of skilled workers for private sector and government.
- **Track 3: Federal Cybersecurity Workforce Structure (Lead: OPM).** Personnel management functions, to include defining cybersecurity jobs in the federal government and skills and competencies required. New strategies to ensure federal agencies attract, recruit, and retain skilled employees to accomplish cybersecurity missions.
- **Track 4: Cybersecurity Workforce Training and Professional Development (Tri-Leads: DoD, ODNI, DHS).** Cybersecurity training and professional development required for federal government civilian, military, and contractor personnel.
  - Subtrack 1: General IT Use (Co-Leads: DHS, Federal CIO Council)
  - Subtrack 2: IT Infrastructure, Operations, Maintenance, and Information Assurance (Co-Leads: DoD, DHS)

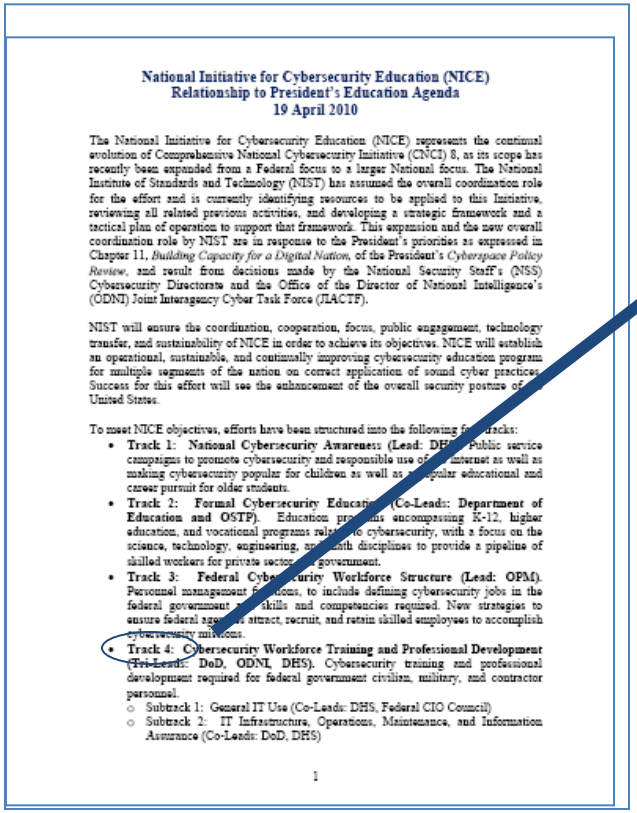
1

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Rollout Experience: The story we had to tell

Helpful to highlight the comprehensive nature of NICE Framework

Made up of multiple components, NICE Component 4 focuses on the standards and development of the Federal Cyber Workforce



National Initiative for Cybersecurity Education (NICE)
Relationship to President's Education Agenda
19 April 2010

The National Initiative for Cybersecurity Education (NICE) represents the continual evolution of Comprehensive National Cybersecurity Initiative (CNCI) 8, as its scope has recently been expanded from a Federal focus to a larger National focus. The National Institute of Standards and Technology (NIST) has assumed the overall coordination role for the effort and is currently identifying resources to be applied to this Initiative, reviewing all related previous activities, and developing a strategic framework and a tactical plan of operation to support that framework. This expansion and the new overall coordination role by NIST are in response to the President's priorities as expressed in Chapter 11, *Building Capacity for a Digital Nation*, of the President's *Cyberspace Policy Review*, and result from decisions made by the National Security Staff's (NSS) Cybersecurity Directorate and the Office of the Director of National Intelligence's (ODNI) Joint Interagency Cyber Task Force (JIACTF).

NIST will ensure the coordination, cooperation, focus, public engagement, technology transfer, and sustainability of NICE in order to achieve its objectives. NICE will establish an operational, sustainable, and continually improving cybersecurity education program for multiple segments of the nation on correct application of sound cyber practices. Success for this effort will see the enhancement of the overall security posture of the United States.

To meet NICE objectives, efforts have been structured into the following four tracks:

- **Track 1: National Cybersecurity Awareness (Lead: DHS).** Public service campaigns to promote cybersecurity and responsible use of the internet as well as making cybersecurity popular for children as well as a popular educational and career pursuit for older students.
- **Track 2: Formal Cybersecurity Education (Co-Leads: Department of Education and OSTP).** Education programs encompassing K-12, higher education, and vocational programs related to cybersecurity, with a focus on the science, technology, engineering, and math disciplines to provide a pipeline of skilled workers for private sector and government.
- **Track 3: Federal Cybersecurity Workforce Structure (Lead: OPM).** Personnel management functions, to include defining cybersecurity jobs in the federal government and skills and competencies required. New strategies to ensure federal agencies attract, recruit, and retain skilled employees to accomplish cybersecurity missions.
- **Track 4: Cybersecurity Workforce Training and Professional Development (Co-Leads: DoD, ODNI, DHS).** Cybersecurity training and professional development required for federal government civilian, military, and contractor personnel.
  - Subtrack 1: General IT Use (Co-Leads: DHS, Federal CIO Council)
  - Subtrack 2: IT Infrastructure, Operations, Maintenance, and Information Assurance (Co-Leads: DoD, DHS)

1

Component 4: Cybersecurity Workforce Training and Professional Development

- Functional Area 1: General IT Use
- Functional Area 2: IT Infrastructure, Operations, Maintenance, and Information Assurance
- Functional Area 3: Domestic Law Enforcement and Counterintelligence
- Functional Area 4: Specialized Cybersecurity Operations

This effort reaches across the Federal Government with included support from DHS, OSTP, ODNI, NSA, DoD,

What are Competency Models? – Nuts and Bolts

CYBER ROLE

Cybersecurity Tester: The Cybersecurity Tester provides compliance-based security testing leveraging automated tools. The Cybersecurity Tester assists in the preparation, development, modification, and management of security products in support of the C&A process. The Cybersecurity Tester provides technical analysis and automated scans to assess their completeness and identify system vulnerabilities and weaknesses.

CYBER SKILLS

- Systems Requirements Analysis
- Testing
- Vulnerability Assessment
- Threat Assessment
- Penetration Testing
- Certification & Accreditation
- Secure Network Design

BEHAVIORAL INDICATORS

THREAT ASSESSMENT: Identifies the impact of circumstances or events with the potential to harm the enterprise

VULNERABILITY ASSESSMENT: Uses knowledge of the types and techniques of Cyber exploitation and attack (e.g.,

TESTING: Performs in-depth, end-to-end testing to ensure secure design and development are in alignment with

SYSTEMS REQUIREMENTS ANALYSIS: Translates functional security requirements into secure design technical and operational specifications. Reviews requirements documentation to determine security impact and requirements. Conducts security risk assessments and business impact analyses to detect weaknesses and depth/breadth of security controls needed. Evaluates current state of security systems, processes, and controls. Performs gap analyses and provides recommendations for gap mitigation.

Proficiency Level 1	Proficiency Level 2	Proficiency Level 3
▸ Performs technical planning, system integration, verification and validation, and supportability and effectiveness analyses for total systems ▸ Analyzes all levels of total system products to include: acquisition, concept, design, test, installation, operation, maintenance, and disposal ▸ Translate operational requirements into technical requirements ▸ Organizes and analyzes stated requirements into categories throughout the system lifecycle such as functionality, usability, performance, operational, security, etc. ▸ Proficient at using a requirements management tool (e.g.. DOORS) ▸ Identifies and documents security requirements	▸ Leads the definition and flow-down functional, performance, and design requirements ▸ Performs functional analysis, timeline analysis, requirements allocation, and interface definition studies to translate customer requirements into hardware and software specifications ▸ Distinguishes testable requirements ▸ Conducts gap analyses between requirements and proposed architecture to identify security performance and other weaknesses in the system ▸ Verifies security requirements through collaboration with DAA/IA/Engineering & Systems Administration ▸ Conducts vulnerability & risk assessment analyses	▸ Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements ▸ Interprets mission objective and applies knowledge to requirements and implementations ▸ Advices customer of gaps in security policy and guidance; provides recommendations ▸ Monitors industry developments and evolving instruction/policy/guidance on IT security concerns ▸ Oversees large-scale requirements development and management efforts to include the definition of new requirements and the implementation of changes to existing requirements.

Example

PERFORMANCE STANDARDS

CYBER SKILL & PROFICIENCY STANDARDS	PERFORMANCE LEVEL		
	INT	EXP	FEL
Systems Requirements Analysis	2	3	3
Testing	2	3	3
Vulnerability Assessment	1	2	3
Threat Assessment	2	2	2
Penetration Testing	1	2	2
Certification & Accreditation	1	2	2
Secure Network Design	1	1	2

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Applying the NICE Framework

DHS SPECIFIC CYBER ROLE

Cybersecurity Tester: The Cybersecurity Tester provides compliance-based security testing leveraging automated tools. The Cybersecurity Tester assists in the preparation, development, modification, and management of security products in support of the C&A process. The Cybersecurity Tester provides technical analysis and automated scans to assess their completeness and identify system vulnerabilities and weaknesses.

SPECIALTY AREAS

- Systems Requirements Planning
- Test and Evaluation
- Investigation
- Computer Network

Selected by Component SMEs from NICE Framework Specialty Areas

BEHAVIORAL INDICATORS

THREAT ASSESSMENT: Identifies the impact of circumstances or events with the potential to harm the enterprise

VULNERABILITY ASSESSMENT: Uses knowledge of the types and techniques of Cyber exploitation and attack (e.g.,

TESTING: Performs in-depth, end-to-end testing to ensure secure design and development are in alignment with

Built by SMEs with alignment to respective NICE Framework KSAs

Proficiency Level 1	Proficiency Level 2	Proficiency Level 3
▸ Performs technical planning, system integration, verification and validation, and supportability and effectiveness analyses for total systems ▸ Analyzes all levels of total system products to include: acquisition, concept, design, test, installation, operation, maintenance, and disposal ▸ Translate operational requirements into technical requirements ▸ Organizes and analyzes stated requirements into categories throughout the system lifecycle such as functionality, usability, performance, operational, security, etc. ▸ Proficient at using a requirements management tool (e.g.. DOORS) ▸ Identifies and documents security requirements	▸ Leads the definition and flow-down functional, performance, and design requirements ▸ Performs functional analysis, timeline analysis, requirements allocation, and interface definition studies to translate customer requirements into hardware and software specifications ▸ Distinguishes testable requirements ▸ Conducts gap analyses between requirements and proposed architecture to identify security performance and other weaknesses in the system ▸ Verifies security requirements through collaboration with DAA/IA/Engineering & Systems Administration ▸ Conducts vulnerability & risk assessment analyses	▸ Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements ▸ Interprets mission objective and applies knowledge to requirements and implementations ▸ Advices customer of gaps in security policy and guidance; provides recommendations ▸ Monitors industry developments and evolving instruction/policy/guidance on IT security concerns ▸ Oversees large-scale requirements development and management efforts to include the definition of new requirements and the implementation of changes to existing requirements.

PERFORMANCE STANDARDS

CYBER SKILL & PROFICIENCY STANDARDS	PERFORMANCE LEVEL		
	INT	EXP	FEL
Systems Requirements Planning	2	3	3
Test and Evaluation	2	3	3
Investigation	1	2	3
Computer Network Defense	2	2	2

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Impact of DHS use of NICE Framework

- Accelerated role specific model development cycle time
- Establishing consistency in terminology across all DHS agencies and components
- Alignment with NICE efforts and future NICE related programs
- Real time feedback from field on framework back to NICE

Exercise 2: Linking Training To the Framework

Why map competencies to training courses?

- Effectiveness
  - ensure that training has “right” content at right level to support needed competencies
  - optimize usefulness of training – enable a robust number of variables to be used for search capabilities to enable very targeted searches to identify applicable/relevant training
- Efficiency – allocate training resources to most benefit
  - eliminate unnecessary redundancy in courses
  - facilitate use of courses to greatest extent possible

Guiding principles

- Competencies and other job-related information to course mappings, in addition to all other required training course information, are an important foundation
- Completing the mapping according to common lexica and taxonomies adds exponentially greater value
- Ideally mapping is done by Subject Matter Experts
- Mapping is not just an exercise – especially in time of increasing scarcity of resources

Process - Mapping Existing Courses to Job Information

- 1st Identify courses to be mapped. May start with a mission critical occupation (e.g., cybersecurity) or by IC element (e.g., DIA)
- 2nd Ensure information about the course is available so that it can be accurately mapped (e.g., has learning objectives documented)
- 3rd Process of successive approximations - - map all fields to the greatest extent possible and with the highest level of consistency/accuracy
- 4th Review and establish a quality assurance process

Session Format

- Linking Courses: What You'll Need
- Example
- Group Exercise

What do you need?

"Things"

- The Cybersecurity Workforce Framework
  - *Must have*
    - Specialty areas with complete descriptions
    - KSAs/Competencies
    - Job titles (helpful for SMEs)

- Training Courses
  - *Must have*
    - Title
    - Description
    - Other data considered in aggregate
      - Objectives
      - Target audience
      - Pre-requisites
      - Number in a series (e.g., 1 of 6)
- Worksheets to record linkages

What do you need?

"People"

- Subject Matter Experts
  - *Must have*
    - Knowledge of course content OR
    - Can become expert in course content through
      - Review of materials
      - Audit course
  - Ideal SME is the ISD or instructor of that training
  - Preferably 2-3 SMEs
    - Supports reliability & validity of linkages
- Facilitator
  - *Must have*
    - Familiarity with the process, purpose
    - Ability to guide SME, either
      - In person
      - Remotely

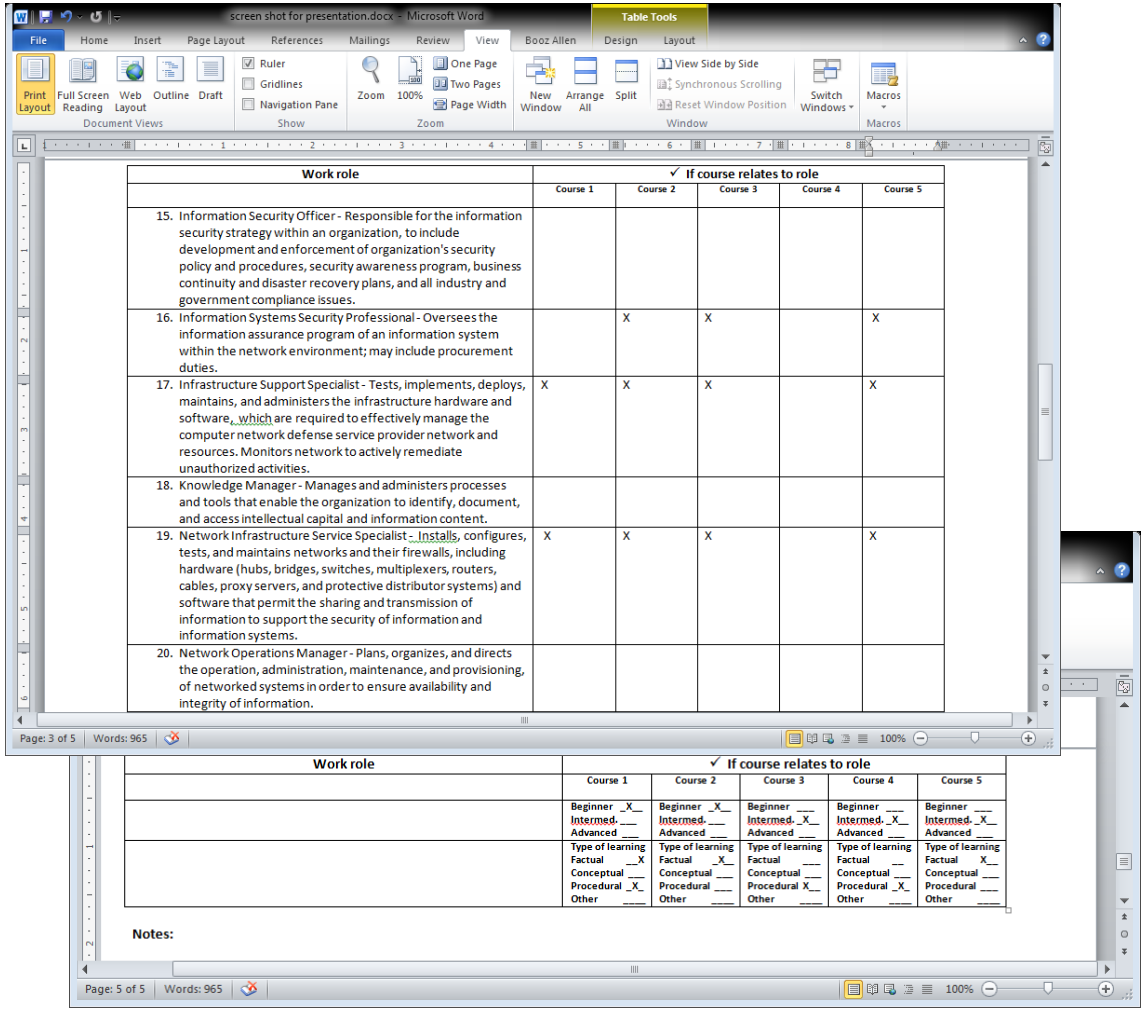
Example from a Facilitated Session

The output shown here came from a facilitated SME session with a cybersecurity training provider from academia

These samples illustrate a portion of the populated worksheet from Step 1 of the process.

Links are shown between six courses and four specialty areas (formerly "work roles")

Note: SMEs were also asked to indicate the level of the intended audience for each course, and type of learning



screen shot for presentation.docx - Microsoft Word

Work role	✓ If course relates to role				
	Course 1	Course 2	Course 3	Course 4	Course 5
15. Information Security Officer - Responsible for the information security strategy within an organization, to include development and enforcement of organization's security policy and procedures, security awareness program, business continuity and disaster recovery plans, and all industry and government compliance issues.					
16. Information Systems Security Professional - Oversees the information assurance program of an information system within the network environment; may include procurement duties.		X	X		X
17. Infrastructure Support Specialist - Tests, implements, deploys, maintains, and administers the infrastructure hardware and software, which are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	X	X	X		X
18. Knowledge Manager - Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.					
19. Network Infrastructure Service Specialist - Installs, configures, tests, and maintains networks and their firewalls, including hardware (hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of information to support the security of information and information systems.	X	X	X		X
20. Network Operations Manager - Plans, organizes, and directs the operation, administration, maintenance, and provisioning, of networked systems in order to ensure availability and integrity of information.					

Page: 3 of 5 | Words: 965

Work role	✓ If course relates to role				
	Course 1	Course 2	Course 3	Course 4	Course 5
	Beginner _X_ Intermed. ___ Advanced ___	Beginner _X_ Intermed. ___ Advanced ___	Beginner ___ Intermed. _X_ Advanced ___	Beginner ___ Intermed. _X_ Advanced ___	Beginner ___ Intermed. _X_ Advanced ___
	Type of learning Factual __X Conceptual ___ Procedural _X_ Other ___	Type of learning Factual _X_ Conceptual ___ Procedural ___ Other ___	Type of learning Factual ___ Conceptual ___ Procedural X__ Other ___	Type of learning Factual ___ Conceptual ___ Procedural _X_ Other ___	Type of learning Factual X__ Conceptual ___ Procedural ___ Other ___

Notes:

Page: 5 of 5 | Words: 965

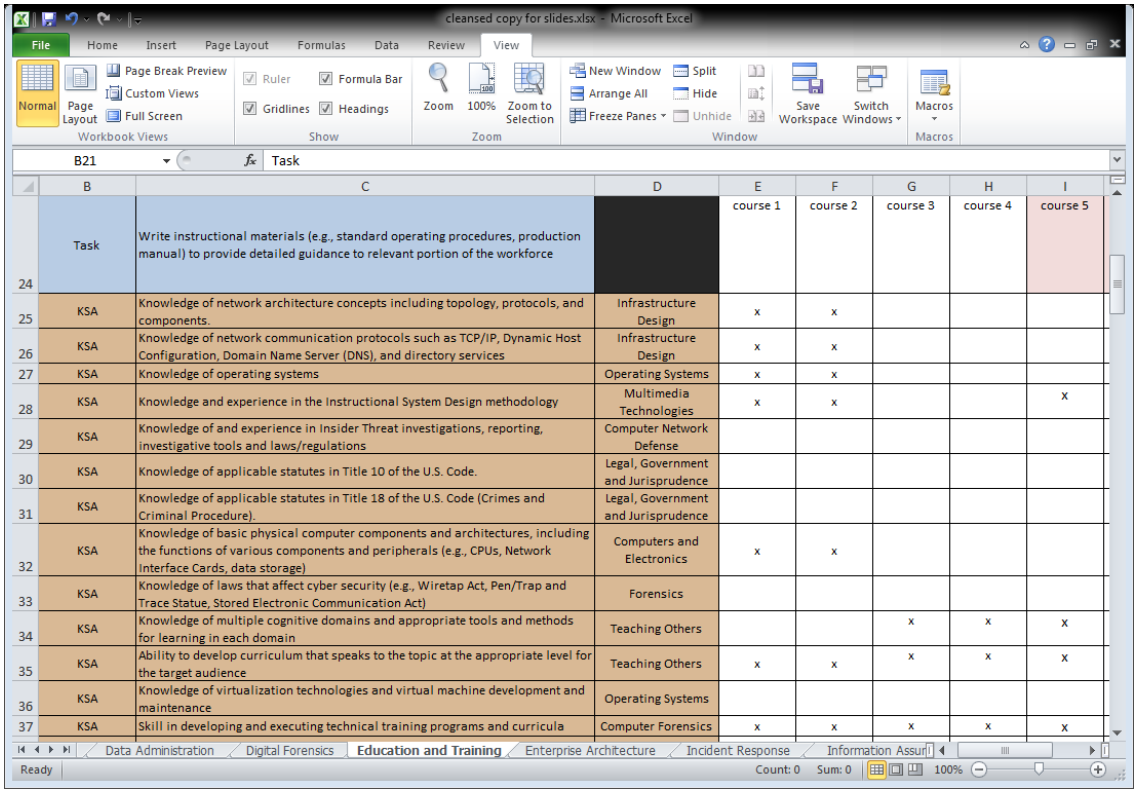
Example from a Facilitated Session continued…

This is an example of the populated framework completed during Step 2 of the process.

This sample illustrates that several of the provider's courses support the KSAs within the Specialty Area "Education and Training"

Note: Several of these courses support multiple KSAs within this specialty area

These linkages, captured in this worksheet, are then entered into the online Cybersecurity Training Catalog



	B	C	D	E	F	G	H	I
24	Task	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce		course 1	course 2	course 3	course 4	course 5
25	KSA	Knowledge of network architecture concepts including topology, protocols, and components.	Infrastructure Design	x	x			
26	KSA	Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services	Infrastructure Design	x	x			
27	KSA	Knowledge of operating systems	Operating Systems	x	x			
28	KSA	Knowledge and experience in the Instructional System Design methodology	Multimedia Technologies	x	x			x
29	KSA	Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/regulations	Computer Network Defense					
30	KSA	Knowledge of applicable statutes in Title 10 of the U.S. Code.	Legal, Government and Jurisprudence					
31	KSA	Knowledge of applicable statutes in Title 18 of the U.S. Code (Crimes and Criminal Procedure).	Legal, Government and Jurisprudence					
32	KSA	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage)	Computers and Electronics	x	x			
33	KSA	Knowledge of laws that affect cyber security (e.g., Wiretap Act, Pen/Trap and Trace Statue, Stored Electronic Communication Act)	Forensics					
34	KSA	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain	Teaching Others			x	x	x
35	KSA	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience	Teaching Others	x	x	x	x	x
36	KSA	Knowledge of virtualization technologies and virtual machine development and maintenance	Operating Systems					
37	KSA	Skill in developing and executing technical training programs and curricula	Computer Forensics	x	x	x	x	x

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Now Let's Try It…

- Your Table Group Will Test the Linkage Process
- Scenario-based Exercise
- Supporting Materials
- We'll Answer Questions
- Time

Task Guidance

- To begin, focus on 1 specialty area
- Using the Framework, take a close look at the KSAs that comprise that specialty area
- Apply your “expertise” (the course information provided) to identify those KSAs that you think are covered in the course
- On the worksheet, write in the KSAs you have identified
- Repeat the process, selecting KSAs for the remaining 2 specialty areas

Wrap up

- How did you do?
- The actual linkages are…

Call to Action

- Help advance the Framework!
  - Provide your input for what we missed, either current or future-oriented
- Adopt the Cybersecurity Workforce Framework
  - If you have existing competency data for cybersecurity within your organization, first map to the framework and then adopt the new labels and definitions
- Volunteer to be a Linkage Expert for Cataloging Cybersecurity Training
  - Work with us to get your courses cataloged and linked to the Framework
- Spread the Word
  - Promote awareness and adoption across the federal government and the Nation