Introduction to NICE Cybersecurity Workforce Framework

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

• The need for understanding the Cybersecurity Workforce
• Introduction to the Cybersecurity Workforce Framework
• The Framework’s intended purpose and use
• Case Study: DHS Pilot Implementation
• Next steps
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....
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 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
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)
Framework Categories

The Framework organizes cybersecurity into seven high-level categories, each comprised of several specialty areas.
## 7 Categories – Each Comprising Several Specialty Areas

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

"So…What else do I get?"
### 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 Systems Security
- Information System 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.....

<table>
<thead>
<tr>
<th>Competency</th>
<th>KSA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Assurance:</strong></td>
<td>Skill in determining how a security system should work.</td>
</tr>
<tr>
<td>Knowledge of methods and</td>
<td>Knowledge of security management</td>
</tr>
<tr>
<td>procedures to protect</td>
<td>Knowledge of Information Assurance principles and tenets.</td>
</tr>
<tr>
<td>information systems and data</td>
<td></td>
</tr>
<tr>
<td>by ensuring their availability,</td>
<td></td>
</tr>
<tr>
<td>authentication, confidentiality</td>
<td></td>
</tr>
<tr>
<td>and integrity.</td>
<td></td>
</tr>
<tr>
<td><strong>Risk Management:</strong></td>
<td>Knowledge of risk management processes, including steps and methods for assessing risk.</td>
</tr>
<tr>
<td>Knowledge of the principles,</td>
<td>Knowledge of network access and authorization (e.g. PKI)</td>
</tr>
<tr>
<td>methods, and tools used for</td>
<td>Skill in, assessing the robustness of security systems and designs.</td>
</tr>
<tr>
<td>risk assessment and mitigation,</td>
<td></td>
</tr>
<tr>
<td>including assessment of failures</td>
<td></td>
</tr>
<tr>
<td>and their consequences.</td>
<td></td>
</tr>
<tr>
<td><strong>System Life Cycle:</strong></td>
<td>Knowledge of system lifecycle management principals.</td>
</tr>
<tr>
<td>Knowledge of systems life cycle</td>
<td>Knowledge of how system components are installed, integrated and</td>
</tr>
<tr>
<td>management concepts used to</td>
<td>optimized.</td>
</tr>
<tr>
<td>plan, develop, implement,</td>
<td>Skill in designing the integration of hardware and software solutions.</td>
</tr>
<tr>
<td>operate and maintain information</td>
<td></td>
</tr>
<tr>
<td>systems.</td>
<td></td>
</tr>
</tbody>
</table>
## Framework Taxonomy

<table>
<thead>
<tr>
<th>Label</th>
<th>Definition</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>A generalized grouping of specialty areas</td>
<td>Can have one or more unique specialty areas associated with a category</td>
</tr>
<tr>
<td>Category</td>
<td></td>
<td>•Belongs to one and only one cybersecurity category</td>
</tr>
<tr>
<td>Specialty Area (SA)</td>
<td>Defines specific areas of specialty within the cybersecurity domain</td>
<td>•Can have any number of unique tasks and KSAs associated with it</td>
</tr>
<tr>
<td>Task</td>
<td>Defines high-level activities that codify a specialty area</td>
<td>•Belongs to one and only one cybersecurity specialty area</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•Tasks are not linked individually to competencies/KSAs</td>
</tr>
<tr>
<td>Competency</td>
<td>A measurable pattern of knowledge, skills, abilities, or other characteristics that individuals need to succeed and that can be shown to differentiate performance.</td>
<td>•One or more KSAs are assigned to each competency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•The same competency is likely to be needed across multiple specialty areas</td>
</tr>
<tr>
<td>KSA</td>
<td>Defines a specific knowledge, skill, ability.</td>
<td>•Assigned to one or more specialty areas</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•Each KSA has exactly one competency associated with it</td>
</tr>
</tbody>
</table>
Intended Use of the Framework… *what you have and what is still needed*
Framework Provided Basis for all Human Capital Actions

• Workforce Baseline Studies – Understand Capabilities (strengths and gaps)
• Position Descriptions
• Hiring Actions (vacancy notices, interviews, assessments, etc.)
• Organizing Training Inventories/Catalogs
• Identify Training Gaps and Needs
• Curriculum and Certification Program Development
• Professional Development Roadmaps
• Professional Standards
• Succession Management
How Do I Use the Framework to Describe My Job

- While the Framework is organized in a very structured way to ensure it would be comprehensive, it is intended to be used in a very flexible way.
  - Consider the content of the Framework as the universal library of things that describe the work and work requirements of cybersecurity
  - Combine the content in any way needed to describe specific jobs or groups of jobs within your organization
  - Recommend beginning by picking the KSAs or tasks that describe what you are after and then get the associated competencies
  - Use the library to do the work across the human capital lifecycle (position descriptions, capture capabilities, catalog training, etc.)
  - Do NOT create new competencies or other library items in isolation! If you feel some concept or a specific KSA is missing...let us know through the NICE portal
Human Capital Data Beyond Competencies and KSAs

To have a comprehensive understanding of the cybersecurity workforce, additional human capital data, beyond the competencies and KSAs data, is needed.

Establishing a complete set of human capital data standards, including personnel transaction type data, is essential to comprehensively understanding the cybersecurity workforce.
Case Study: DHS Pilot Implementation
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.
“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 Capability 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

<table>
<thead>
<tr>
<th>Competency</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penetration Testing</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 National Initiative for Cybersecurity Education (NICE) represents the continued 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 operations to support that framework. This expansion and the new overall coordination role by NIST is in response to the President’s priorities as expressed in Czarna 11, Building Capacity for a Digital Nation, the President’s 2012 Cybersecurity Policy Review, and results from decisions made by the National Security Staff’s (NSS) Cybersecurity Directorate and the Office of the Director of National Intelligence’s (ODNI) Joint Cyber Task Force (JCTF).

NIST will assume the coordination, cooperation, and funding of cybersecurity education program for multiple segments of the nation on current applications 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 generate cybersecurity awareness and knowledge in all sectors of the American economy. The campaign will include awareness of issues such as phishing, social engineering, and the importance of good cybersecurity practices.
- **Track 2: Formal Cybersecurity Education (Co-Leads: Department of Education and CISA).** 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: ODNI).** Personal management functions, to include defining cybersecurity jobs in the federal government, and skills and competencies required. New strategies to attract federal agency staff, recruit and retain skilled employees to accomplish cybersecurity missions.
- **Track 4: Cybersecurity Workforce Training and Professional Development (Lead: DoD, OMB, 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)
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
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**

- 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
- Translates 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
- Advises 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**

<table>
<thead>
<tr>
<th>CYBER SKILL &amp; PROFICIENCY STANDARDS</th>
<th>PERFORMANCE LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>INT</td>
</tr>
<tr>
<td>Systems Requirements Analysis</td>
<td>2</td>
</tr>
<tr>
<td>Testing</td>
<td>2</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>1</td>
</tr>
<tr>
<td>Threat Assessment</td>
<td>2</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>1</td>
</tr>
<tr>
<td>Certification &amp; Accreditation</td>
<td>1</td>
</tr>
<tr>
<td>Secure Network Design</td>
<td>1</td>
</tr>
</tbody>
</table>
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.

SPECIALITY AREAS

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

Selected by Component SMEs from NICE Framework Specialty Areas

BEHAVIORAL INDICATORS

Built by SMEs with alignment to respective NICE Framework KSAs

<table>
<thead>
<tr>
<th>CYBER SKILL &amp; PROFICIENCY STANDARDS</th>
<th>PERFORMANCE LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Requirements Planning</td>
<td>INT</td>
</tr>
<tr>
<td>Test and Evaluation</td>
<td>INT</td>
</tr>
<tr>
<td>Investigation</td>
<td>INT</td>
</tr>
<tr>
<td>Computer Network Defense</td>
<td>INT</td>
</tr>
</tbody>
</table>

- 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
- Translates 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
- Performs gap analyses and makes recommendations for gap mitigation depth/breadth of security controls needed. Evaluates current state requirements. Conducts security risk assessments and business impact analyses.
- Conducts vulnerability & risk assessment analyses
- Verifies security requirements through collaboration with DAA/IA/Engineering & Systems Administration
- Conducts technical planning, system design, integration, verification and validation, and supportability and effectiveness analyses for total systems
- 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 from non-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
- Advises 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.
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
Call to Action

• 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

• Help advance the Framework!
  – Provide your input for what we missed, either current or future-oriented

• Spread the Word
  – Promote awareness and adoption across the federal government and the Nation