

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



Cybersecurity Workforce Structure, Training, and Professional Development within NICE



8/17/11

Peggy Maxson and Angela Curry, DHS/NCSD/CEO

THE PAST

Training the existing federal cyber workforce in specialized skills and ensuring a federal cybersecurity workforce pipeline for the future.

Initiative #8, Expand Cyber Education

60 Day Cyber Review

Building Capacity for a Digital Nation

- Promote cybersecurity risk awareness for all citizens;
 - Build an education system that will enhance understanding of cybersecurity and allow the United States to retain and expand upon its scientific, engineering, and market leadership in information technology;
 - Expand and train the workforce to protect the Nation's competitive advantage; and
 - Help organizations and individuals make smart choices as they manage risk.
- 60-Day Cyber Review*

National Initiative for Cybersecurity Education

THE VISION

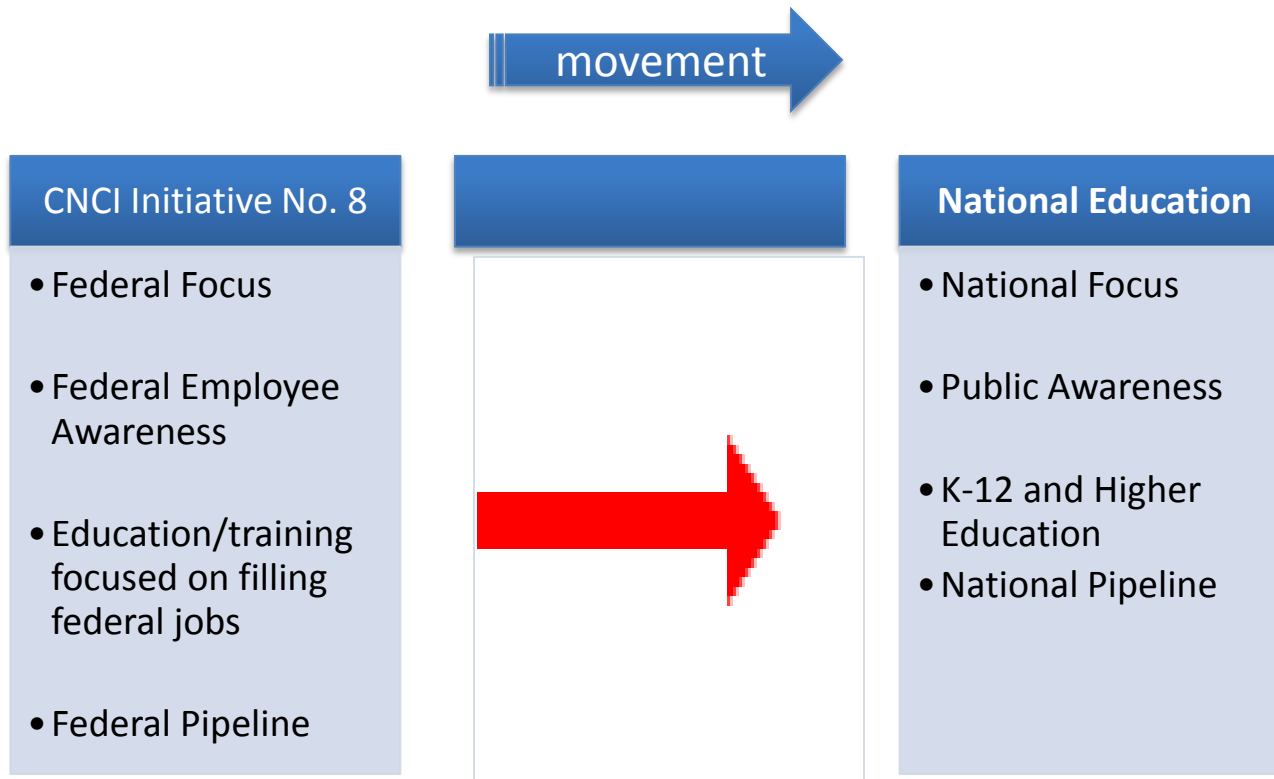
“...a national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms, and to build a digital workforce for the 21st century.”



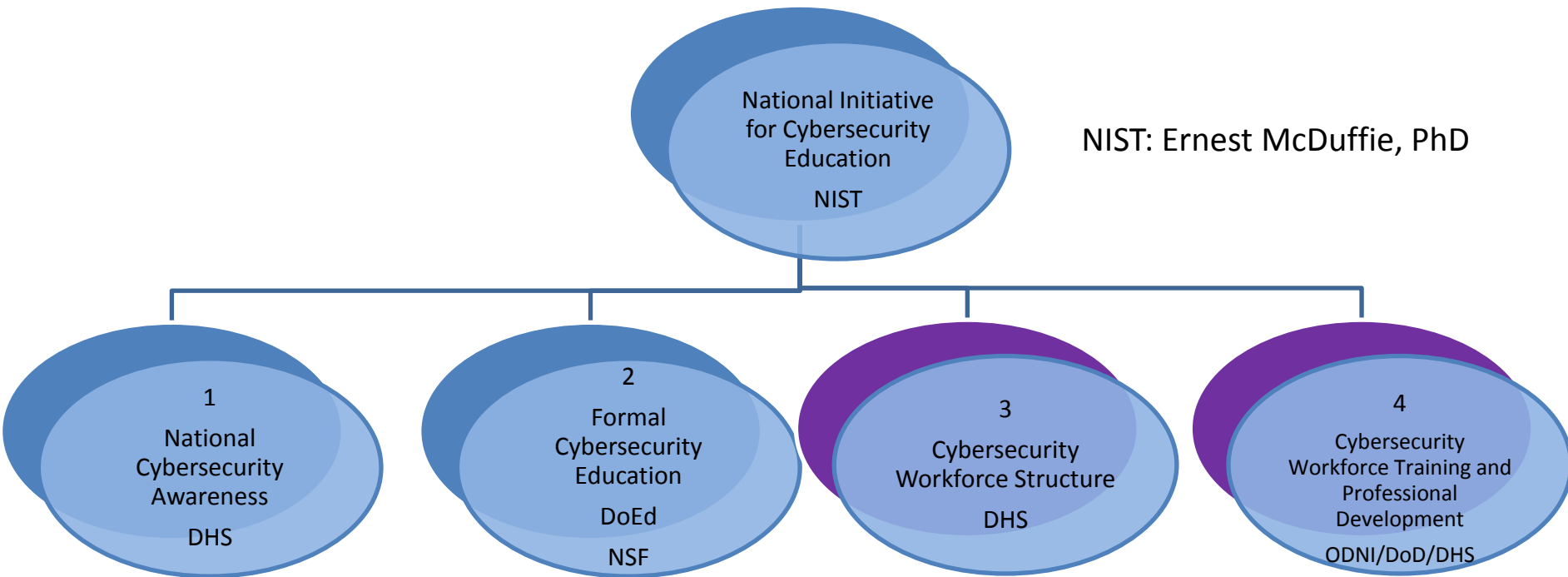
President Barack Obama, 29 May 2009

EXPANDED FOCUS OF NICE

movement



NICE Governance Structure



NIST: Ernest McDuffie, PhD

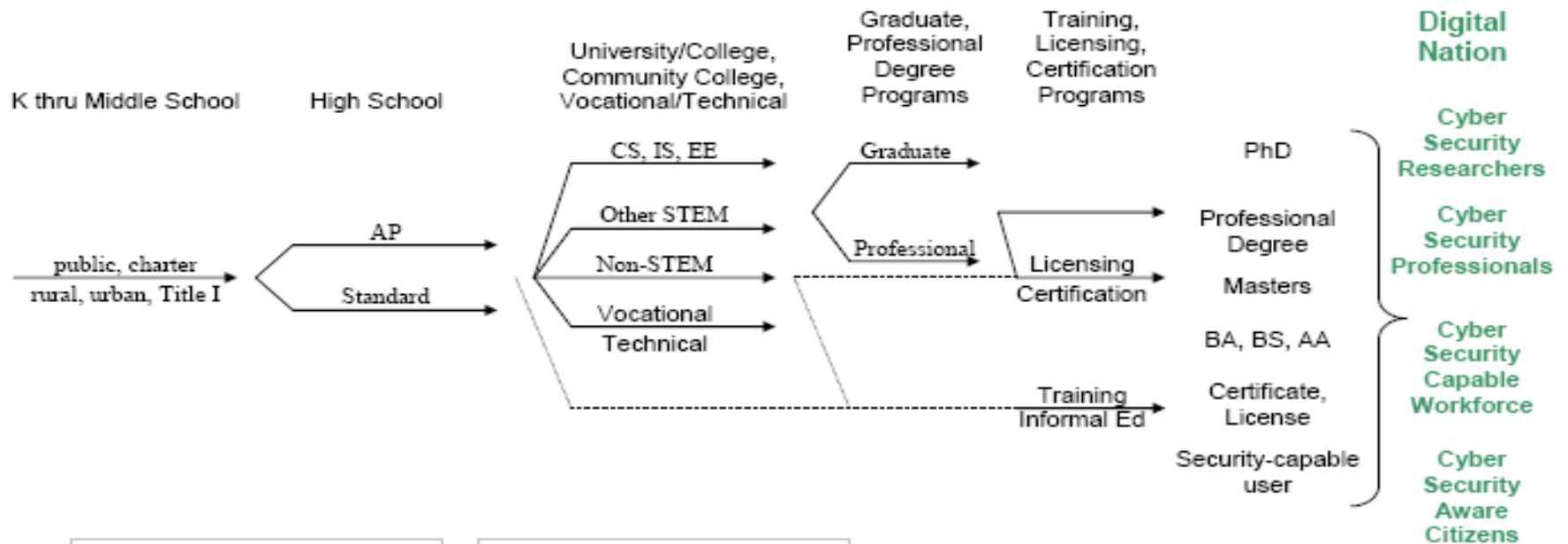
DHS:
Tim Fraser
Kristina Dorville

ED: Michael Lach
NSF: Jan Cuny, PhD

DHS: Anji Curry

ODNI: Jane Homeyer,
PhD
DOD: John Mills
DHS: Peggy Maxson

The Pipeline



Pipeline Stakeholders:

- Students
- Parents
- Teachers
- Educational Institutions
- State, Local Government
- Professional Organizations
- Commercial Sector
- Federal Government

Pipeline Substrates:

- Curriculum
- Ontologies, Taxonomies
- Standards
- Teacher Preparation
- Public Awareness
- Education Technologies
- Science and Practice of Learning

Cybersecurity Workforce Training and Professional Development

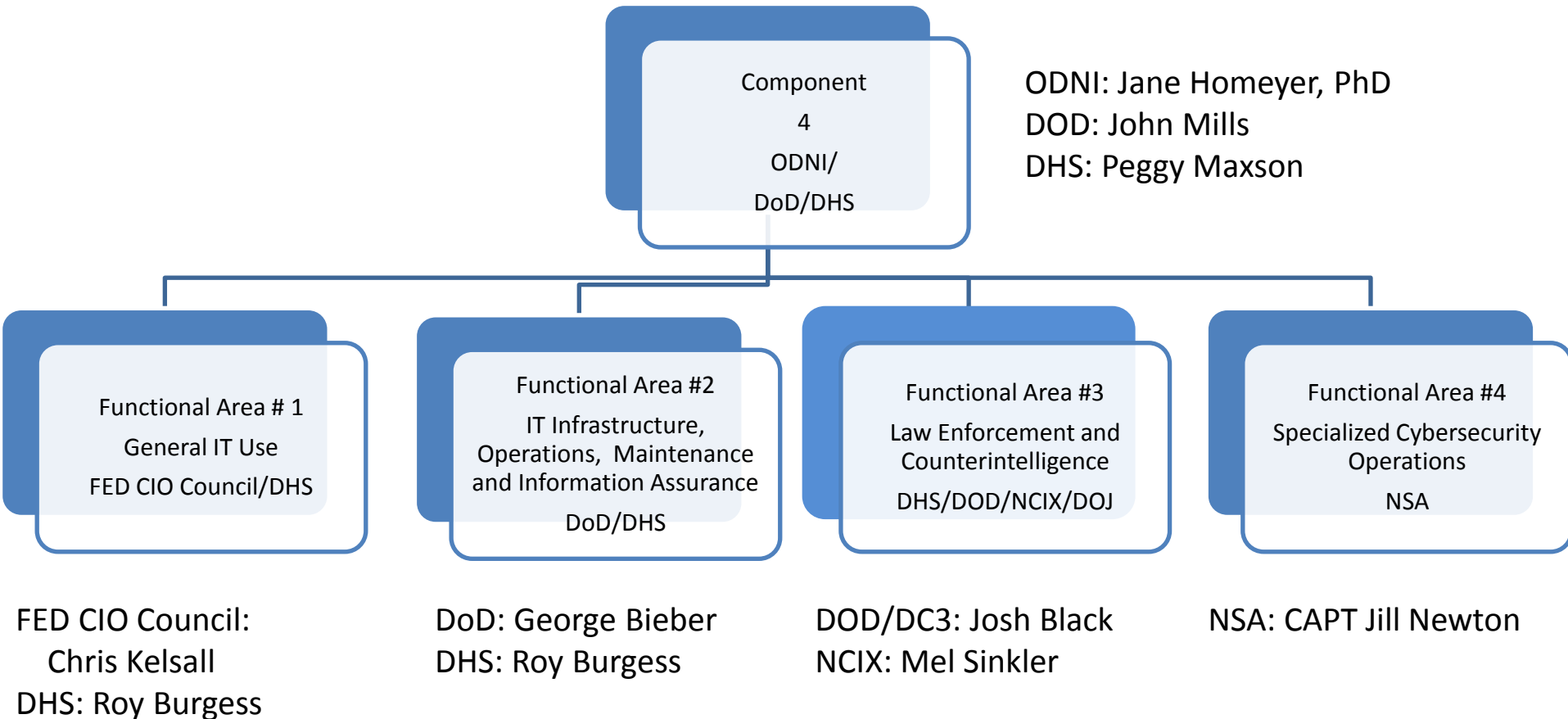
Tri-Leads: DHS – Peggy Maxson

DOD – John Mills

ODNI/CHCO – Jane Homeyer, Ph.D.



Cybersecurity Workforce Training and Professional Development



Task Overview

Task 1 – Population Review - Defining the Workforce – The Framework

Task 2 – Training Catalog – Identifying the training per level

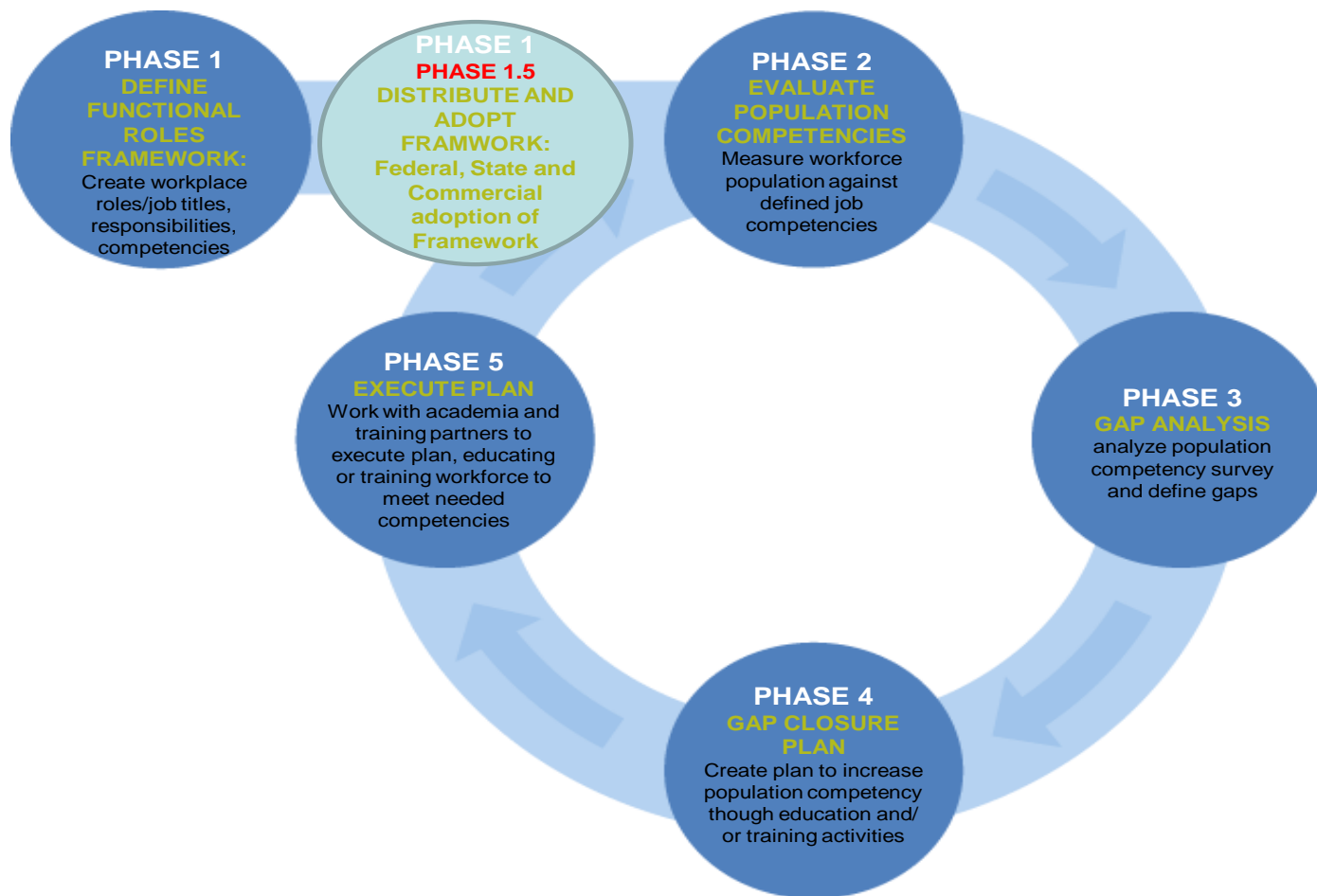
Task 3 – Workforce Baseline Study – assess the quality

Task 4 – Workforce & Training Analysis - Identification of gaps

Task 5 – Professional Development Roadmaps – the pipeline

Task 6 - Communication

The Nation's Workforce Health Measurement Process



Multiple federal efforts

NIST SP 800-16, Rev. 1 (NIST)

Development of a Department of Defense Cybersecurity Workforce Framework and Preliminary Training Gap Analysis, July 2010 (DOD)

Federal Cybersecurity Workforce Transformation Working Group Report on Cybersecurity Competencies, July 2010 (DOD, DHS)

IT Security Workforce Matrix Project (FED CIO IT Workforce Committee)

Competency Model for Cybersecurity, 16 Feb 2011 (OPM – NICE Track 3)

Comprehensive National Cyber Initiative #8 Expand Cyber Education Activities (Leads: DHS, NSA)

ISS LOB Tier 1 Awareness Training Initiative (Lead: DHS)

ISS LOB Tier 2 Role-Based Training Initiative (Lead: DHS)

Essential Body of Knowledge (Lead: DHS)

CNSS Education Training and Awareness Working Group & Training Standards (Lead: CNSS)

Focusing all National Efforts

- NICE effort serves as the focal point for existing and future cybersecurity workforce development initiatives.
- Compilation of all previous Federal efforts; collaborating with SLT, academia and private sector.
- A single touch point for the nation that is recognized as the “go to” point for cybersecurity education and training.
- NICE, partnering with all of those who strive to improve the capabilities and effectiveness of cybersecurity professionals, can begin to build to the future.

Focusing all National Efforts

- Federal – guidelines and standards
- State, Local, Tribal – encourage participation in building and common acceptance
- Academia - collaborate and ensure best practices, encourage common adoption or crosswalk
- Industry – collaborate and ensure best practices, encourage common adoption or crosswalk

Category: Operate and Maintain

Functional Role: Systems Security Analyst

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. Implement and/or integrate security measures for use in system(s) and ensure that system designs incorporate security configuration guidelines.
5. Discover organizational trends with regard to the security posture of systems.
6. etc.

Competency	KSAs
Information Assurance: Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	Skill in designing countermeasures to identified security risks.
	Knowledge of existing IA security principles, policies, and procedures.
	Knowledge of IT security principles and methods, such as firewalls, DMZ, and encryption.
Risk Management: Knowledge of the principles, methods, and tools used for risk assessment and mitigation, including assessment of failures and their consequences.	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
	Knowledge of network access and authorization (e.g., public key infrastructure).
	Skill in assessing the robustness of security systems and designs.
Systems Life Cycle: Knowledge of systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems.	Knowledge of embedded systems.
	Knowledge of how system components are installed, integrated, and optimized.
	Skill in designing the integration of hardware and software solutions.
Etc.	Etc.

Color Key:

Track 3

Track 4

Both

NICE Cybersecurity Specialties Framework

The 31 Cybersecurity Specialties:

Securely Provision

- Systems Requirements Planning**
- Systems Development**
- Software Engineering**
- Enterprise Architecture**
- Test and Evaluation**
- Technology Demonstration**
- Information Assurance Compliance**

Operate and Maintain

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

Support

- Legal Advice and Advocacy**
- Education and Training**
- Strategic Planning and Policy Development**

Protect and Defend

- Computer Network Defense Infrastructure Support**
- Vulnerability Assessment and Management**
- Incident Response**
- Computer Network Defense**
- Security Program Management**

Investigate

- Investigation**
- Digital Forensics**

Operate and Collect

- Collection Operations**
- Cyber Operations Planning**
- Cyber Operations**

Analyze

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

Framework Development

✓ over 20 Federal Departments and Agencies support framework development to include DOS, ED, DOL, OMB, OPM, DOD, DOJ, NIST, DIA, CIA, NSA, FBI, DNI, NSF, DOD/DC3, NCIX, and various components of DHS (NPPD, TSA, USSS, Coast Guard, ICE, CBP, CIS, DHS OI&A)

In addition, NICE has worked very closely with non-profit and governmental organizations to socialize the framework:

- ✓ 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)
- ✓ Consortium of Certification Organizations
- ✓ Institute for Information Infrastructure Protection (I3P)
- ✓ Association for Computing machinery (ACM)
- ✓ Institute of Electrical and Electronics Engineers (IEEE)

Framework example

The 31 Cybersecurity Specialties:

Securely Provision

- Systems Requirements Planning**
- Systems Development**
- Software Engineering**
- Enterprise Architecture**
- Test and Evaluation**
- Technology Demonstration**
- Information Assurance Compliance**

Operate and Maintain

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

Support

- Legal Advice and Advocacy**
- Education and Training**
- Strategic Planning and Policy Development**

Protect and Defend

- Computer Network Defense Infrastructure Support**
- Vulnerability Assessment and Management**
- Incident Response**
- Computer Network Defense**
- Security Program Management**

Investigate

- Investigation**
- Digital Forensics**

Operate and Collect

- Collection Operations**
- Cyber Operations Planning**
- Cyber Operations**

Analyze

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



Framework Definition Example

Specialty

Sample Job Titles

Data Administration - develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

- Data warehouse specialist
- Database developer
- Database administrator
- Data architect
- Information dissemination manager
- Content staging specialist
- Data manager
- Systems operations personnel

Framework Tasks Example

Data Administration	Task	Analyze and define data requirements and specifications
Data Administration	Task	Analyze and plan for anticipated changes in data capacity requirements
Data Administration	Task	Design and implement database systems
Data Administration	Task	Develop and implement data mining and data warehousing programs
Data Administration	Task	Develop data standards, policies, and procedures
Data Administration	Task	Install and configure database management systems software
Data Administration	Task	Maintain assured message delivery systems
Data Administration	Task	Maintain database management systems software
Data Administration	Task	Maintain directory replication services that enables information to replicate automatically from rear servers to forward units via optimized routing
Data Administration	Task	Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required
Data Administration	Task	Manage the compilation, cataloging, caching, distribution, and retrieval of data
Data Administration	Task	Monitor and maintain databases to ensure optimal performance
Data Administration	Task	Perform backup and recovery of databases to ensure data integrity
Data Administration	Task	Provide a managed flow of relevant information (via web-based portals or other means) based on a mission requirements
Data Administration	Task	Provide recommendations on new database technologies and architectures

Framework KSAs Example

Linked to OPM Competency:

Data Administration	KSA	Knowledge of data administration and data standardization policies and standards	Data Management
Data Administration	KSA	Knowledge of data backup and recovery concepts and tool, including different types of backups (e.g., full, incremental)	Computer Forensics
Data Administration	KSA	Knowledge of data mining and data warehousing principles	Data Management
Data Administration	KSA	Knowledge of database management systems, query languages, table relationships, and views	Database Management Systems
Data Administration	KSA	Knowledge of digital rights management	Encryption
Data Administration	KSA	Knowledge of agency LAN/WAN pathways	Infrastructure Design
Data Administration	KSA	Knowledge of enterprise messaging systems and associated software	Enterprise Architecture
Data Administration	KSA	Knowledge of network access and authorization (e.g., public key infrastructure)	Identity Management
Data Administration	KSA	Knowledge of operating systems	Operating Systems
Data Administration	KSA	Knowledge of policy-based and risk adaptive access controls	Identity Management
Data Administration	KSA	Knowledge of query languages such as SQL (structured query language)	Database Management Systems
Data Administration	KSA	Knowledge of sources, characteristics, and uses of the organization's data assets	Data Management
Data Administration	KSA	Knowledge of telecommunications concepts	Telecommunications
Data Administration	KSA	Knowledge of the characteristics of physical and virtual data storage media	Data Management
Data Administration	KSA	Skill in allocating storage capacity in the design of data management systems	Database Administration
Data Administration	KSA	Skill in designing databases	Database Administration
Data Administration	KSA	Skill in developing data dictionaries	Data Management
Data Administration	KSA	Skill in developing data models	Modeling and Simulation
Data Administration	KSA	Skill in developing data repositories	Data Management
Data Administration	KSA	Skill in generating queries and reports	Database Management Systems
Data Administration	KSA	Skill in maintaining databases	Database Management Systems
Data Administration	KSA	Skill in optimizing database performance	Database Administration
Data Administration	KSA	Knowledge of database theory	Data Management

NATIONAL INSTITUTE FOR CYBERSECURITY STUDIES (NICS)

NICS is an implementation tool for the NICE efforts.

Mission

Provide a national resource for the American public for cybersecurity awareness, education and training resources

Goals

1. Build a national resource to elevate cybersecurity awareness and effect a change in the American public to adopt a culture of cyberspace security.
2. Promote cybersecurity education from kindergarten through the post graduate level to nurture the future cybersecurity workforce.
3. Guide the development of cybersecurity standards, training, and professional development to empower and advance cybersecurity personnel.
4. Manage NICS program through NICS Program Management Office (PMO).

THREE ELEMENTS OF THE NICS APPROACH



ADVISORY BOARD

Comprised of representatives from government, academia and industry, the advisory board provides recommendations to NICS for the development of cybersecurity awareness, education and career training.



VIRTUAL UNIVERSITY

Enables federal, state, local and tribal government employees access online training resources that are optimized for cybersecurity workforce development.



WEB PORTAL

Makes cybersecurity information and resources more readily available to the workforce and promotes greater collaboration among cybersecurity educators and employers.

Draft NICS Portal Homepage

NICS

National Institute for Cybersecurity Studies

Search this site... 

NEWS & EVENTS

CYBERSECURITY AWARENESS

EDUCATION

TRAINING

CAREERS

COMMUNITY

ABOUT NICS

CYBER DISCOVERY CAMP

hosted by
Louisiana Tech University

July 11-16, 2011

[Find out more](#)

1 2 3 4 5



Cybersecurity News

[Cybertheft and the U.S. Economy](#)
Council on Foreign Relations | August 11, 2011

[Former CIA Counter-Terror Chief: Al Qaeda will go cyber](#)
ABC News | August 11, 2011

[Anonymous allegedly threatens to 'kill' Facebook](#)
ComputerWorld | August 10, 2011 09:50 AM

[China says it was targeted in 500,000 cyberattacks](#)
The Huffington Post | August 9, 2011 07:49 AM

[Anonymous hacker collective hits rural law enforcement](#)
Homeland Security News Wire | August 9, 2011 07:49 AM

[More News](#)  [RSS Feed](#)

Cybersecurity Terms A-Z



Learn basic terminology and find out how you can become more cybersecurity aware.

Cybersecurity Degree Programs



Find the right cybersecurity program for you in the NICS Cybersecurity Degree Programs Directory.

Upcoming Training

Oct 9 [SANS Baltimore 2011](#)
Baltimore, MD
SANS Commercial

Oct 17 [Certified Information Systems Security Professional \(CISSP\) Preparation](#)
Live Online
UMBC Training Centers Commercial

Oct 18 [Grid SecCon 2011](#)
New Orleans, LA
SANS Commercial

Oct 23 [SANS Chicago 2011](#)
Chicago, IL
SANS Commercial

Nov 7 [Advanced Training: Control Systems Cyber Security Advanced Training and Workshop](#)
Idaho Falls, Idaho
US CERT Government Employees Only

[More Training](#)  [RSS Feed](#)

Newest Job Postings

Today
[Special Senior Advisor for Cyber Security \(SL\)](#)
Department Of Homeland Security - Washington DC Metro Area, DC

Today
[Sr. Cyber Security Researcher](#) - NEW
Idaho National Laboratory - Idaho Falls, ID

Yesterday
[Cyber Security Engineer](#)
SRA International - Arlington, VA

Yesterday
[Cyber Security/Wireless Research Engineer](#)
Harris Corporation - Herndon, VA

2 days ago
[Cyber Security Operations Engineer](#)
Silverrhino - Alexandria, VA

2 days ago
[Chief Technology Officer](#)
Department Of Homeland Security - Arlington, VA

3 days ago
[Cyber Security - Technical Project Manager](#)

[More Jobs](#)  [RSS Feed](#)

NICS PROJECT TIMELINE

FY
2011

- Validate portal requirements and design
- Portal mockup and start of development

FY
2012

- Establish NICS PMO
- Assemble Advisory Board
- Portal operational

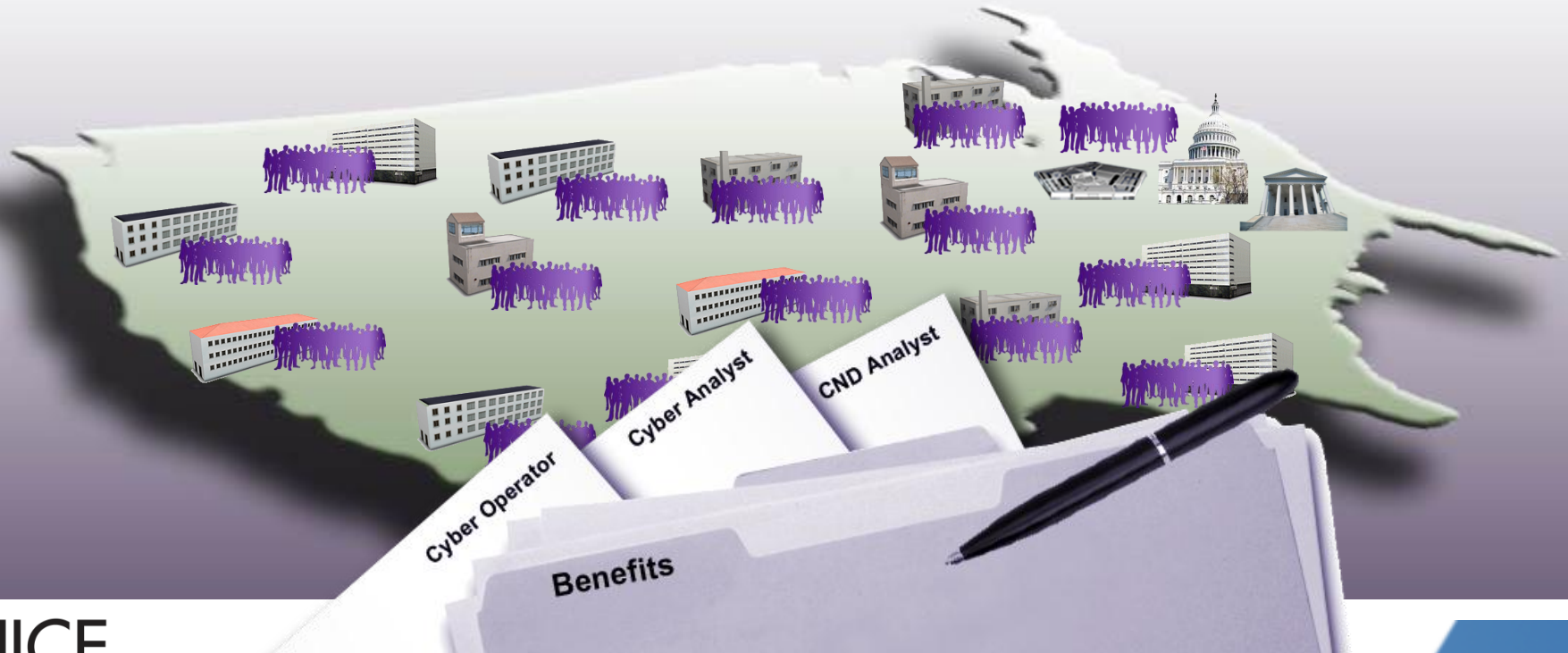
FY
2013

- Pilot State, local, and Tribal Virtual Training Environment
- Expand portal content partnerships
- Continuously update portal content

Cybersecurity Workforce Structure

Lead:

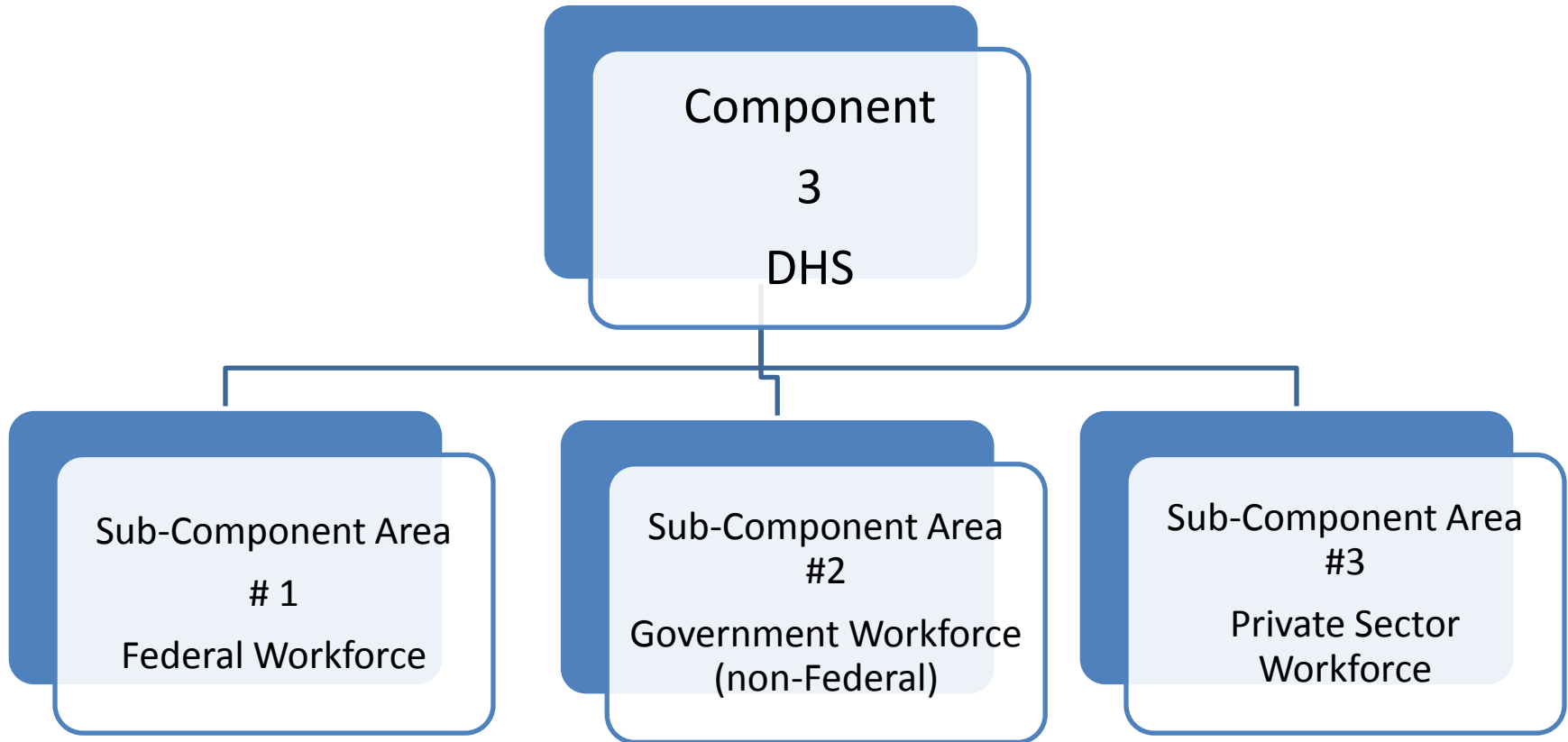
DHS, Angela Curry



Goal of Component 3

Define cybersecurity as a profession, attract, recruit, retain, and establish career paths.

Cybersecurity Workforce Structure



Component 3 Tasks

Task 1 – Need For & Effectiveness of Cybersecurity Professionalization

Task 2 – Cybersecurity Workforce “As Is”

Task 3 – Cybersecurity Workforce “To Be”

Task 4 – Tracking Cybersecurity Workforce Pipeline & Changes

Task 5 – Tracking Workforce Recruitment & Retention Effectiveness

Task 6 – Recommend & Plan to Close Workforce Recruitment & Retention Gaps

Professionalization

- A profession arises when any trade or occupation transforms itself through *"the development of formal qualifications based upon education, apprenticeship, and examinations, the emergence of regulatory bodies with powers to admit and discipline members, and some degree of monopoly rights.*

- Alan Bullock & Stephen Trombley, *The New Fontana Dictionary of Modern Thought*, London: Harper-Collins, 1999, p.689.

Cybersecurity Workforce Structure, Training and Professional Development

... Discussion ...

Tom Ruoff – tom.ruoff@dhs.gov

Peggy Maxson – margaret.maxson@dhs.gov

Angela Curry – angela.curry@dhs.gov

Roy Burgess – roy.burgess@dhs.gov

QUESTIONS?

