NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

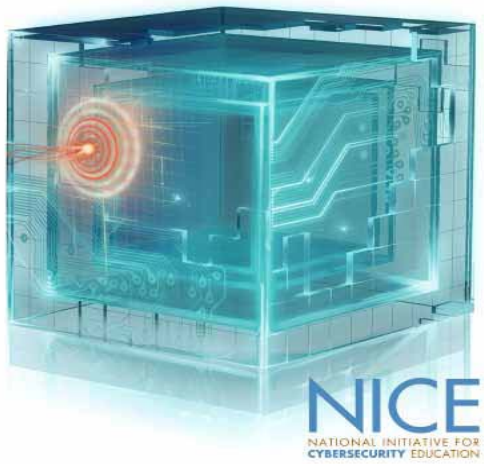
21st Century Cybersecurity Workforce Framework

Peggy Maxson, Director National Cybersecurity Education Strategy
Department of Homeland Security

Outline for Today

- NICE Overview
- Cybersecurity Workforce Definition
- The Pipeline
- The Cybersecurity Workforce Framework
- Framework Activities and Next Steps
- Call to Action

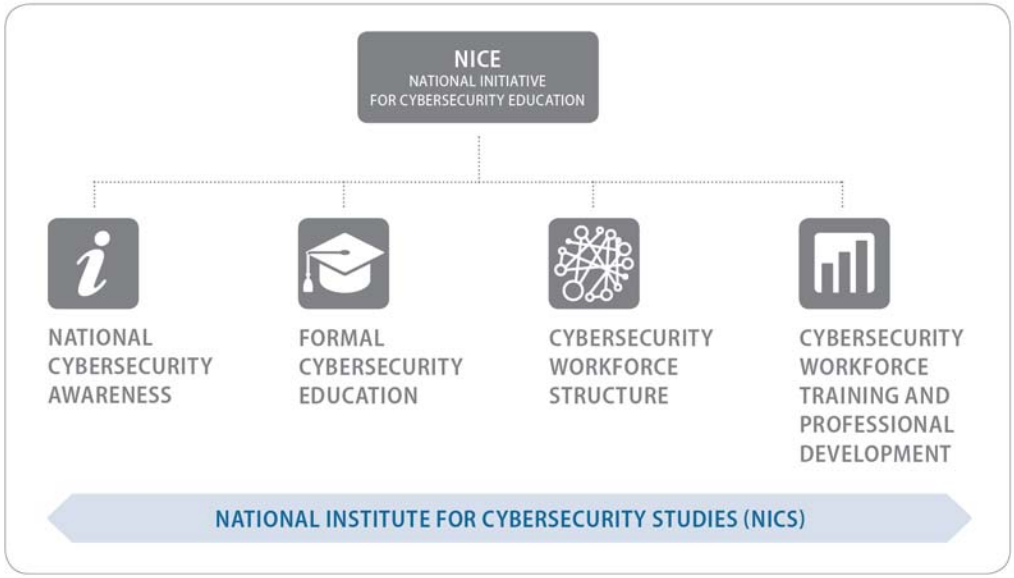
- http://www.nist.gov/nice/framework/



A National Problem

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

NICE was established to create a cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security.

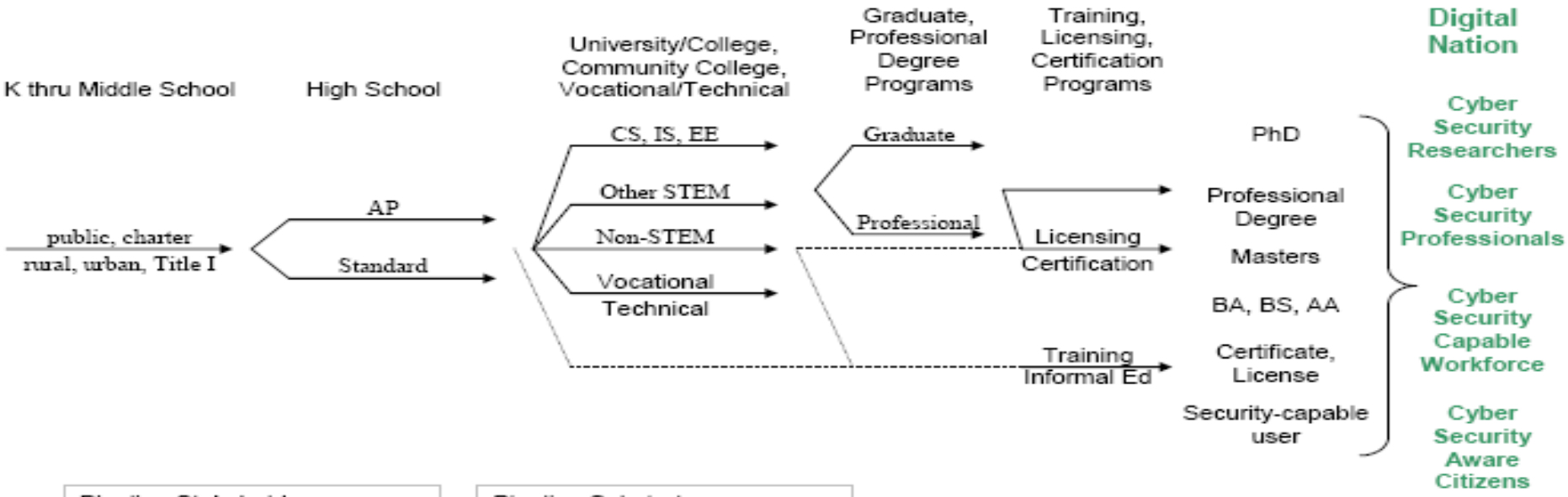


Cybersecurity Career Field

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

Cyberspace Policy Review May 2009

The Pipeline



Pipeline Stakeholders:

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

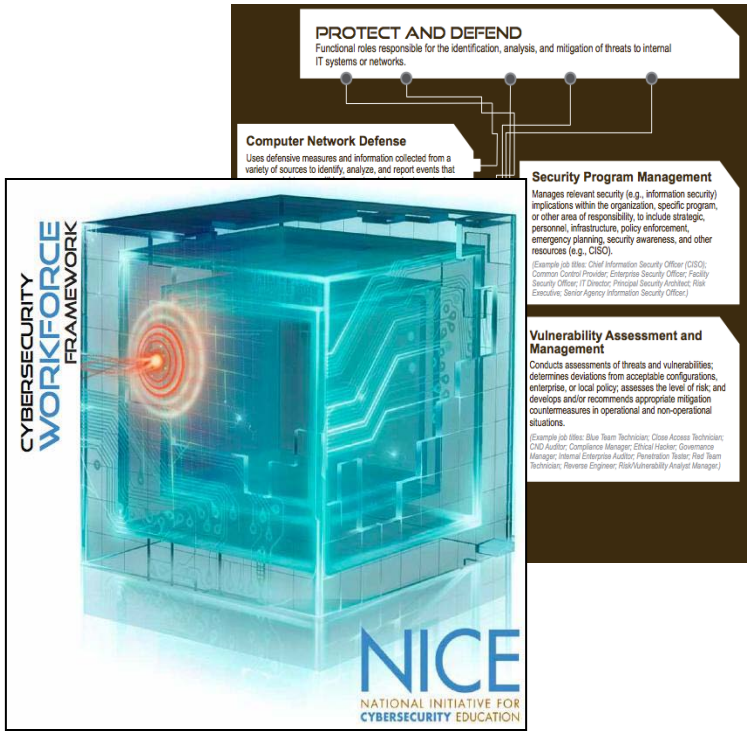
Pipeline Substrates:

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

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

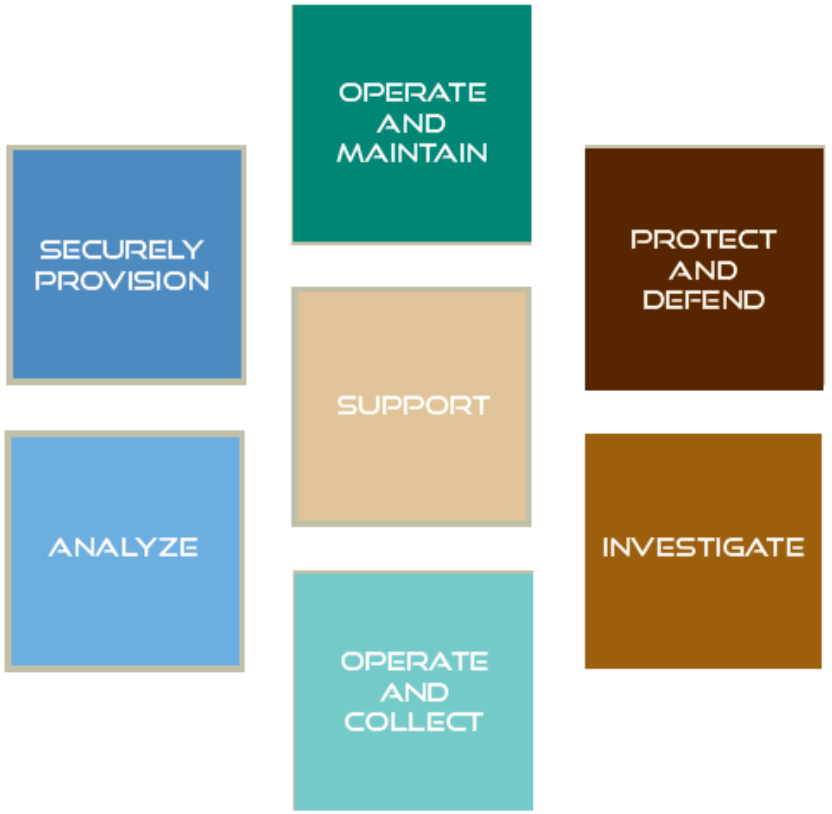
Cybersecurity Workforce Framework

- The NICE Cybersecurity Workforce Framework provides a common language and taxonomy to define cybersecurity work.
- Over 20 Federal Agencies and Departments contributed to the development.
- NICE has worked closely with non-profit and governmental organizations to socialize the framework.
- Framework Taxonomy
  - Cybersecurity Category: A generalized grouping of specialty areas
  - Specialty Area (SA): Defines specialty areas within the cybersecurity domain
  - Competency: A measurable pattern of knowledge, skills, abilities, or other characteristics that individuals need to succeed and that can be shown to differentiate performance
  - KSA: Defines a specific knowledge, skill, or ability
  - Task: Defines a specific task



Framework Categories

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



CYBERSECURITY WORKFORCE FRAMEWORK

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

31 Specialty Areas

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

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

Investigate

- Investigation
- Digital Forensics

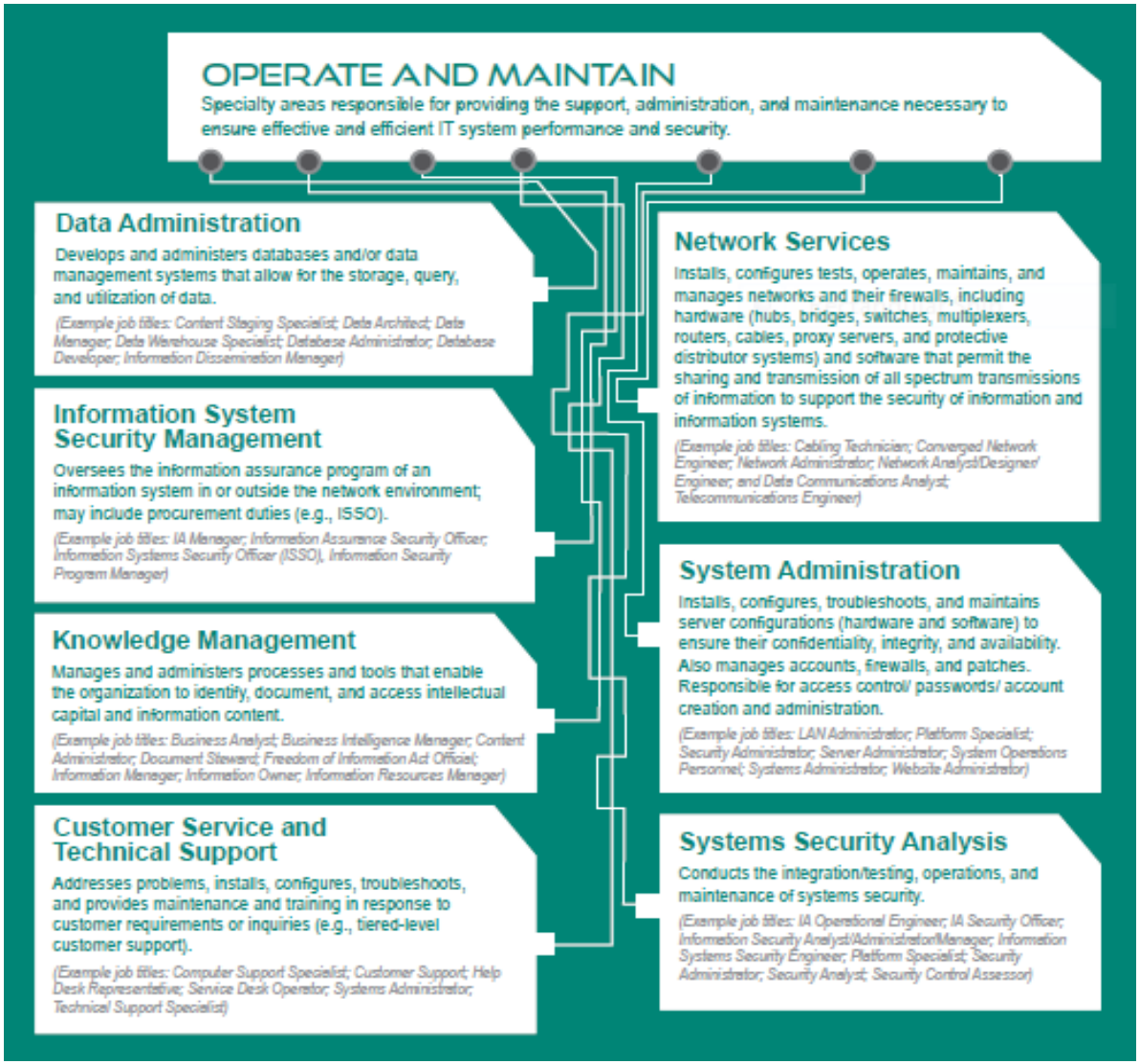
Operate and Collect

- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Analyze

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

Specialty Area Example



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.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION
Component 4: Co-led by DHS / ODNI / DOD

NICE Framework: Provide a common language to define cybersecurity work. Defines specialty areas, KSAs, competencies.

Key Activities: Finalize Framework (Mar 2012), Roll-out to Initial Federal Stakeholders (Jul 2012), Remaining Fed Stakeholders (Jul 2013)*

Training Catalog / NICS: Provide an online resource with a robust training collection mapped to the NICE Framework.

Key Activities: Launch of the NICS Portal (Sep 2012), Launch of the Training Catalog (Mar 2013)*

Workforce Inventory: Identify the current state of the IT workforce, and assess cybersecurity capabilities.

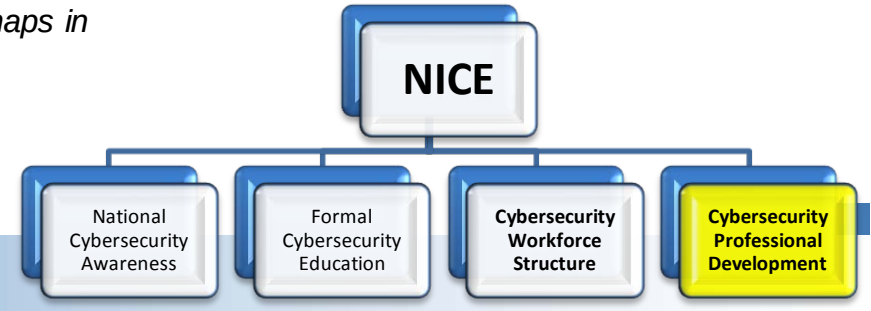
Key Activities: Federal Pilot & Development (Nov 2012), Submit Federal Findings Report (Nov 2012), Federal Metrics Report (Dec 2012)*

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

Key Activities: Workforce Current Training Needs Report (Feb 2013), Training Gap Analysis Report (May 2013)*

Professional Development Roadmaps: Develop resources which depict progression from entry to expert.

Key Activities: Develop and Publish Professional Development Roadmaps in NICS (Dec 2012)*



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

Framework Activities and Next Steps

- The Framework has been available for public review and feedback on the NIST website since September 20, 2011.
- Introduction of the framework occurred at multiple conferences, such as the NICE Workshop in September 2011, the quarterly Software Assurance (SwA) Forum, the Centers for Academic Excellence (CAE) Principals Meeting, and the Department of Navy CIO Conference, to name a few.
- Ten focus groups were conducted with Subject Matter Experts (SMEs) to validate specialty areas, tasks, and KSAs.
- We are compiling feedback, comments, and SME input to produce a revised and finalized Framework by March 31, 2012.
- The Framework will then enter the Office of Management and Budget's (OMB) Legislative Referral Memoranda (LRM) process to coordinate interagency approval.

Call to Action

- Agencies across the Federal Government will begin to align their jobs and positions to this specialty area framework.
- This framework may be chosen by industry, academia, and state, local, tribal government as a model to follow.
- Several products are in development that will aid with the roll-out, such as a users' guide and a speakers' tool-kit.
- With a common structure and lexicon, we can not only better understand the makeup of our cybersecurity population, but also begin to identify the capabilities of those individuals.
- In so doing, we can start to identify and develop the necessary workforce, training and professional development opportunities to help address our growing cybersecurity concerns.
- Help us help you! http://www.nist.gov/nice/framework/