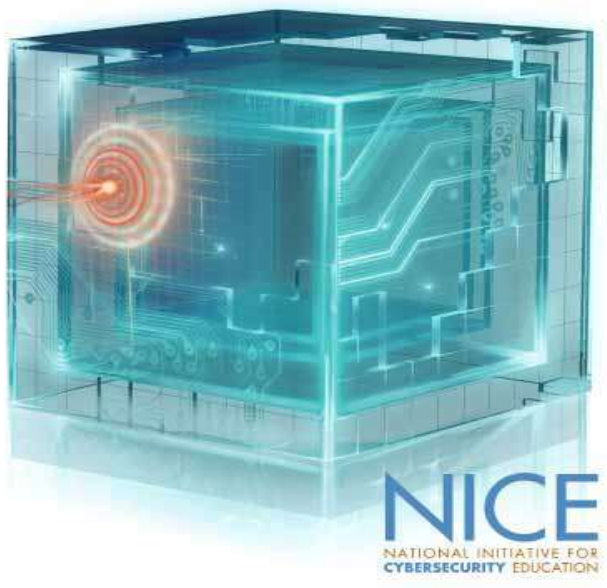
NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE and Framework Overview

Bill Newhouse
NIST NICE Leadership Team
Computer Security Division
Information Technology Lab
National Institute of Standards and Technology

Table of Contents



A National Problem

- The Nation needs greater cybersecurity awareness and more cybersecurity experts.
- There is a lack of communication between government, private industry, and academia.
- Many cybersecurity training programs exist but there is little consistency among programs, and potential employees lack information about the skills needed for jobs.
- Cybersecurity Career development and scholarships are available but uncoordinated, and the resources that do exist are difficult to find.

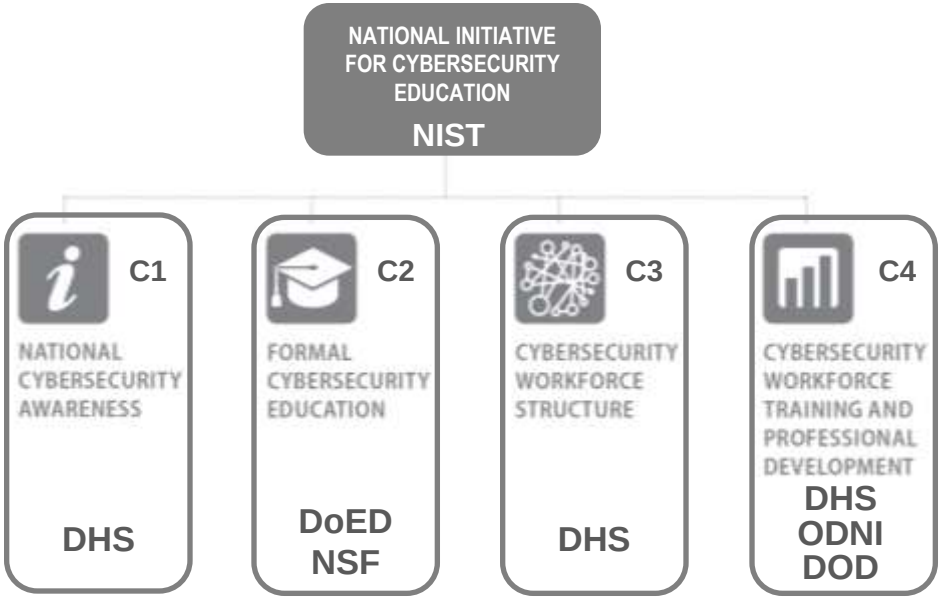
NICE was established in support of the Comprehensive National Cybersecurity Initiative (CNCI) – Initiative 8: Expand Cyber Education – Interim Way Forward and is comprised of over 20 federal departments and agencies.

CYBERSECURITY DEFINITION

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. "

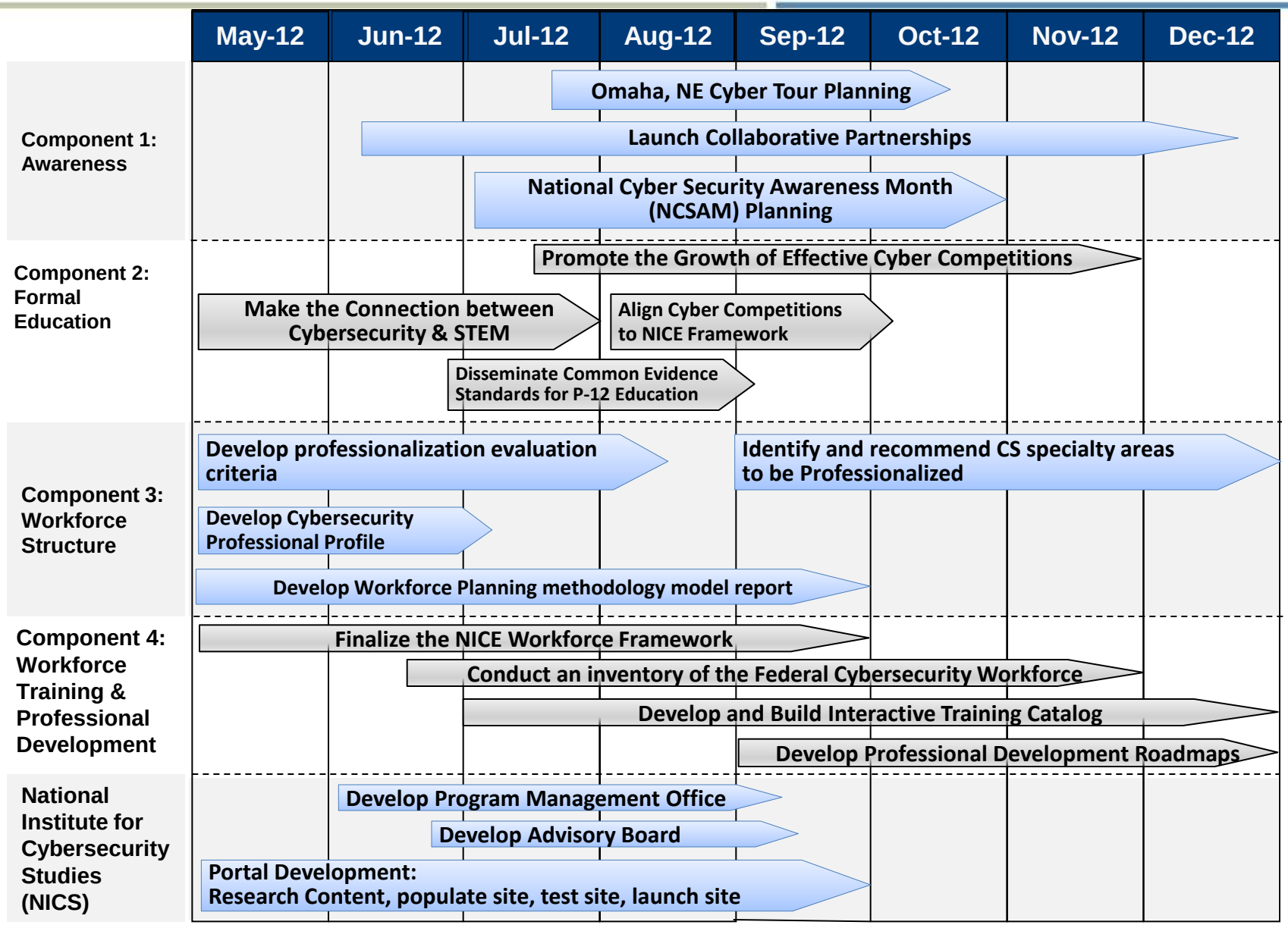
Cyberspace Policy Review May 2009

NICE STAKEHOLDERS AND LEADERSHIP



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Project Timeline Snapshot: May - Dec



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

COMPONENT 4 PROJECTS AND ACTIVITIES

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

- *Key Activities: Framework Finalized (May 2012), LRM Process (August 2012) and Roll-out to Initial Federal Stakeholders (August 2012), and Roll-out to remaining Federal Stakeholders (May 2013)*

Training Catalog / NICS: Provide an online web resource that provides a robust and representative collection of trainings mapped to the NICE Framework.

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

Workforce Inventory: Collect data to baseline and identify the current state of the IT workforce, and assess current cybersecurity capabilities.

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

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

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

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE FRAMEWORK

The NICE Cybersecurity Workforce Framework, which was released in 2011, outlines 31 functional work specialties within the cybersecurity field and is the foundation of the effort.

- The Framework was developed in collaboration with subject matter experts from government, non-profits, academia, and the private sector.
- The Framework organizes cybersecurity into seven high-level categories, each comprised of several specialty areas.
- The Framework has been broadly accepted as a best practice to define the cybersecurity field.

CYBERSECURITY WORKFORCE FRAMEWORK

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.

Component 3: Cybersecurity Talent Management

Talent Management is a holistic view of human capital that includes functions of workforce planning, talent acquisition, talent engagement, talent development, deploying talent, leading talent, and retaining talent.

Component 3 is the Workforce Structure component of NICE and focuses on talent management of cybersecurity professionals. It aims to evaluate the ***professionalization*** of the workforce, recommend ***best practices for forecasting*** future cybersecurity needs, and define national strategies for ***recruitment and retention***.

COMPONENT 3 PROJECTS AND ACTIVITIES

Professionalization: Establish a methodology for identifying cybersecurity areas to be professionalized and provide a central national resource for cybersecurity professionalization.

- *Key Activities: Professionalization analysis and methodology developed (May 2013), Professionalization Implementation Plan Developed (Sept 2013)*

Workforce Planning: Deliver a methodology for accurately forecasting cybersecurity workforces across government, industry, and academia.

- *Key Activities: Cybersecurity Workforce Planning Model Development (Sep 2012), Pilot Program Executed (Jan 2013), National Workforce Planning Methodology Implemented (Apr 2013)*

Recruitment and Retention: Provide, disseminate and maintain a strategy and set of materials for recruiting and retaining cybersecurity professionals at the national level.

- *Key Activities: Cybersecurity Professional Profile (July 2012), Recruitment Plan Published (Apr. 2013), Retention Plan Published (May 2013)*

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

PROFESSIONALIZATION

Work collaboratively with federal agencies, State, Local, Tribal and Territorial governments, industry and academia to recommend professionalization of certain cybersecurity specialty areas. The intent is to recommend professionalization standards and allow industry to set certification or licensing requirements.

Vision and Mission

- The vision of the cybersecurity professionalization project is to be the central national resource for cybersecurity professionalization.
- Its mission is to deliver a methodology for identifying cybersecurity areas for professionalization.

Objective	Deliverables/Activities	Deadline
Research potential professionalization processes, and the impacts of each, by examining the history and procedures of occupations which have professionalized	Historical report of professionalization	April 2012
Analyze need for professionalizing cybersecurity workforce, and, if professionalization is deemed necessary, evaluate which of the 31 cybersecurity specialty areas will be professionalized	Professionalization best practices analysis report	August 2012
	Report identifying specialty areas to be professionalized	November 2012
Provide a set of governance standards for professionalization	Implementation plan for professionalizing existing specialty areas	March 2013
Socialize Professionalization implementation plan with Federal, State, Local, Tribal and Territorial governments and industry	Meeting minutes gaining consensus on the professionalization implementation plan	Ongoing

WORKFORCE PLANNING

Develop scalable and repeatable workforce planning methodologies using leading best practices for the cybersecurity field to plan for future needs; allow organizations to gauge their own cybersecurity workforce planning strengths and weaknesses and provide best practices for improvement.

Vision and Mission

- The vision of the cybersecurity workforce planning project is to be the national resource for cybersecurity workforce planning.
- Its mission is to deliver a methodology for accurately forecasting cybersecurity workforces across government, private sector, and academia.

Objective	Deliverables/Activities	Deadline
Research best practices methodologies for workforce planning	Workforce Planning Methodologies Report	May 2012
Define methodology components for cybersecurity workforce planning	Workforce Planning Methodologies Development Report	September 2012
Perform a Pilot Program for workforce methodology	Results Report on Pilot Program	February 2013
Develop a strategy to conduct a gap analysis of the current cybersecurity workforce	Strategy for gap analysis	May 2013
Socialize Workforce Planning methodology for cybersecurity workforce with Federal, State, Local, Tribal and Territorial (SLTT) governments and industry	Strategy for Implementation Plan for a Full Scale Workforce Planning Methodology	July 2013

ENGAGEMENT OPPORTUNITIES

- Cyber Workforce Inventory Project (May)
- Professionalization Panels (Summer)
- NICE Workshop (October 30 – November 1)
- NICE Framework Data Element

ENGAGEMENT OPPORTUNITIES

- Cyber Workforce Inventory Project (May)
  - Identify participants to join Behavioral Indicator Focus Groups
  - Dates: May 2nd,1:30-3:30pm and May 3rd,3:00-5:00m

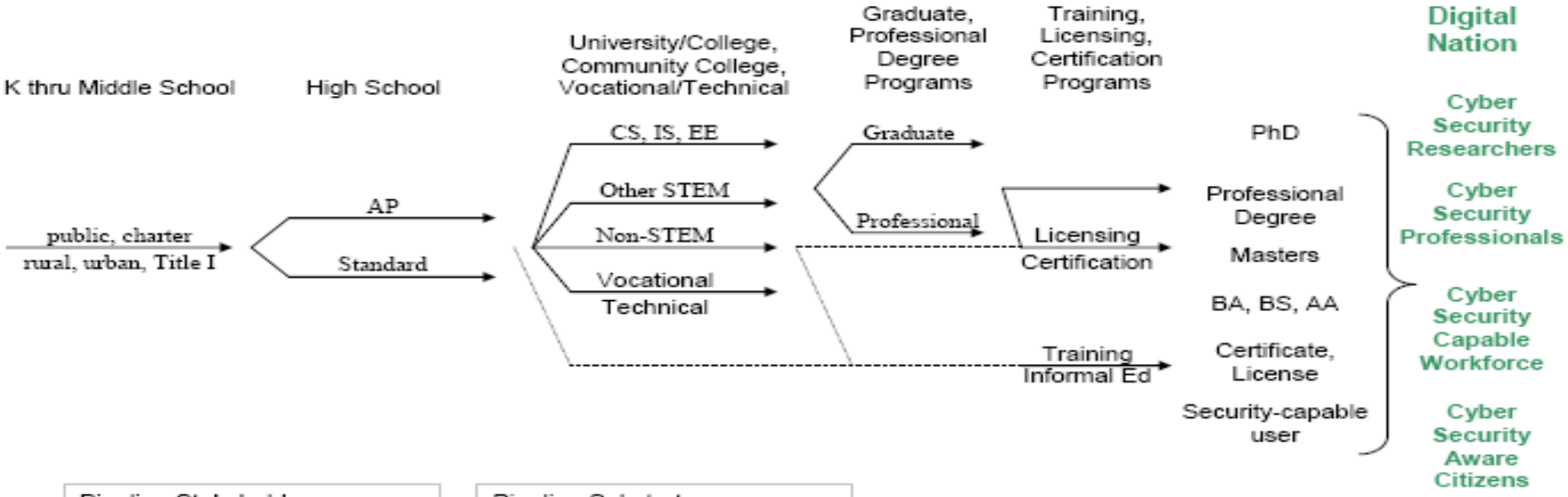
- Professionalization Panels (Summer)
  - Identify Federal representatives to participate

- NICE Workshop (October 30 – November 1)
  - Identify Federal representatives to join panel presentations

- NICE Framework Data Element
  - Establish a working group to implement by August 9, 2012
  - According to the NICE Work Breakdown Structure (WBS), the data element should be implemented by August 9, 2012

BACKUP

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

FRAMEWORK TAXONOMY

Label	Definition	Relationship
Cybersecurity Category	A generalized grouping of specialty areas	Can have one or more unique specialty areas associated with a category
Specialty Area (SA)	Defines specific areas of specialty within the cybersecurity domain	•Belongs to one and only one cybersecurity category •Can have any number of unique tasks and KSAs associated with it
Competency	A measurable pattern of knowledge, skills, abilities, or other characteristics that individuals need to succeed and that can be shown to differentiate performance.	•One or more KSAs are assigned to each competency
KSA	Defines a specific knowledge, skill, ability.	•Assigned to one or more specialty areas •Each KSA has exactly one competency associated with it
Task	Defines a specific task.	•Each task has no competency association

7 CATEGORIES – DEFINED

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.

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

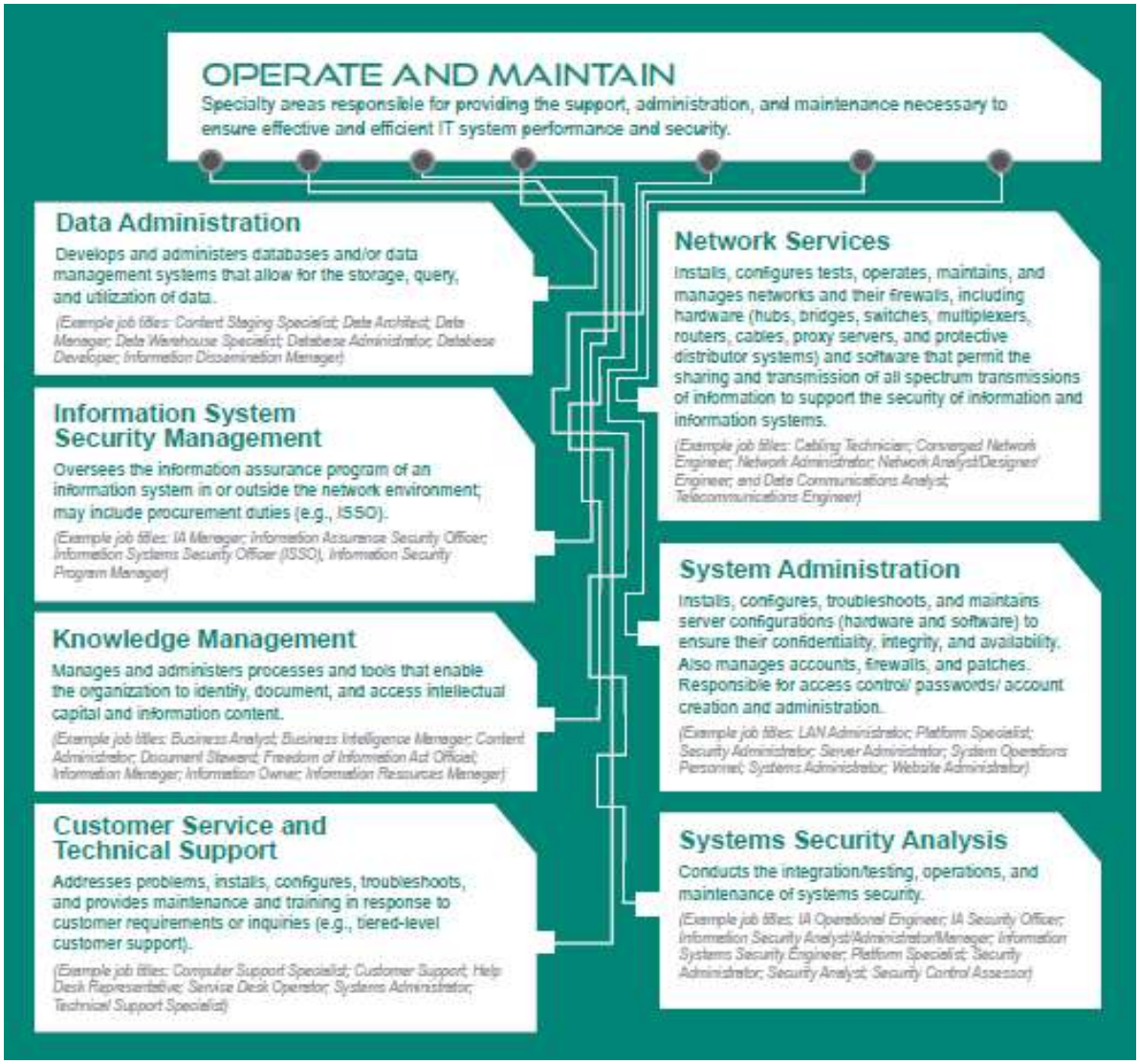
Operate and Collect

- Collection Operations
- Cyber Operations Planning
- Cyber Operations

Analyze

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

SPECIALTY AREAS (SA)



Sample Applications of the Framework

Application of the Framework

- The Framework is intended as a working taxonomy which can be overlaid onto an existing organizational structure and can be customized for specific agency components, or generalized across organizations
- Since the size and scope of cyber workforces widely varies, many organizations may not find a role for each of the 31 specialty areas, but instead may need to combine specialties
- The Framework is comprehensive and inherently flexible, allowing organizations to adapt its content to their human capital and workforce planning needs

- Requires agencies to independently deploy resources to define agency-specific roles and descriptions
- Agencies risk misinterpreting the Framework in their custom applications
- Customized approach is needed for law enforcement and specialized operations applications

- Leverages previous matrix project work and this SME group to define sample framework applications common across agencies
- The 31 specialty areas are combined into broader areas of responsibility often seen in smaller cybersecurity organizations
- The samples are intended to provide a baseline application of the Framework for 80 percent of organizations

DIGITAL FORENSICS & INCIDENT RESPONSE ANALYST

Foundational NIST NICE Specialty Area(s):

Incident Response (p. 13)

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Digital Forensics (p. 18)

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

Federal Digital Forensics & Incident Response Analyst Defined:

The Digital Forensics and Incident Response Analyst performs a variety of highly technical analyses and procedures dealing with the collection, processing, preservation, analysis, and presentation of computer-related evidence, and is responsible for disseminating and reporting cyber-related activities, conducing vulnerability analyses and risk management of computer systems and all applications during all phases of the systems development lifecycle. The Digital Forensics and Incident Response Analyst provides oversight of incident data flow and response, content, preservation of evidence, and remediation, and partners with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets. The Digital Forensics and Incident Response Analyst conducts chain of custody activities between the organization and appropriate law enforcement entities.

INFORMATION SECURITY OFFICER

Foundational NIST NICE Specialty Area(s):

Information Systems Security Management (p. 8)

Oversees the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., ISSO).

Federal Information Systems Security Officer Defined:

The Information Systems Security Officer (ISSO) specializes in the information security within a system and is engaged throughout the systems development life cycle. The ISSO ensures that the appropriate operational posture is maintained for an information system and is responsible for advising system owners and interfacing with users. The ISSO communicates with the business at the system level and understands security threats and vulnerabilities to the operations and the system's environment. The ISSO will typically have the detailed technical expertise necessary to manage the day-to-day security operations of a system. In organizations where the ISSO role is performed by non-government employees, the strategic system decisions are made by the ISSM or CISO.