NICE OVERVIEW
Women's Business and Smart Technology
23 May 2014

- **2008 - Comprehensive National Cybersecurity Initiative #8**

  - "…we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees."

- **2009 - 60-Day Cyber Review**
  - 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;

NICE
NATIONAL INITIATIVE FOR **CYBER**SECURITY EDUCATION

March 2010: NICE formed

"…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

A NATIONAL PROBLEM

- The Nation needs greater cybersecurity awareness.
- The US workforce 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.
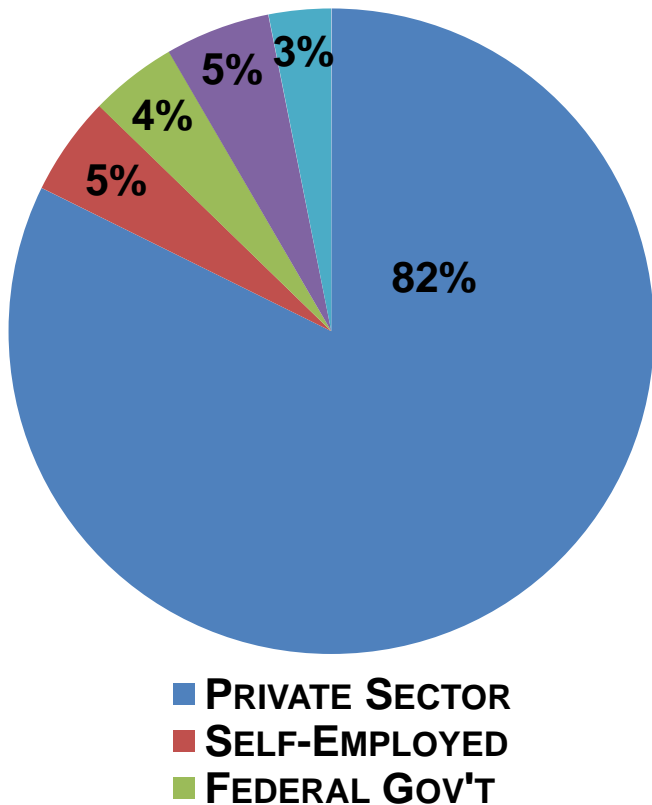- Lack of communication between government, private industry, and academia.

The National Initiative for Cybersecurity Education (NICE) was established to raise national cybersecurity awareness, broaden the pool of cybersecurity workers through strong education programs, and build a globally competitive cybersecurity workforce.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NATIONAL CYBERSECURITY AWARENESS

FORMAL CYBERSECURITY EDUCATION

CYBERSECURITY WORKFORCE STRUCTURE

CYBERSECURITY WORKFORCE TRAINING AND PROFESSIONAL DEVELOPMENT

National Initiative for Cybersecurity Careers and Studies (NICCS)

NICE
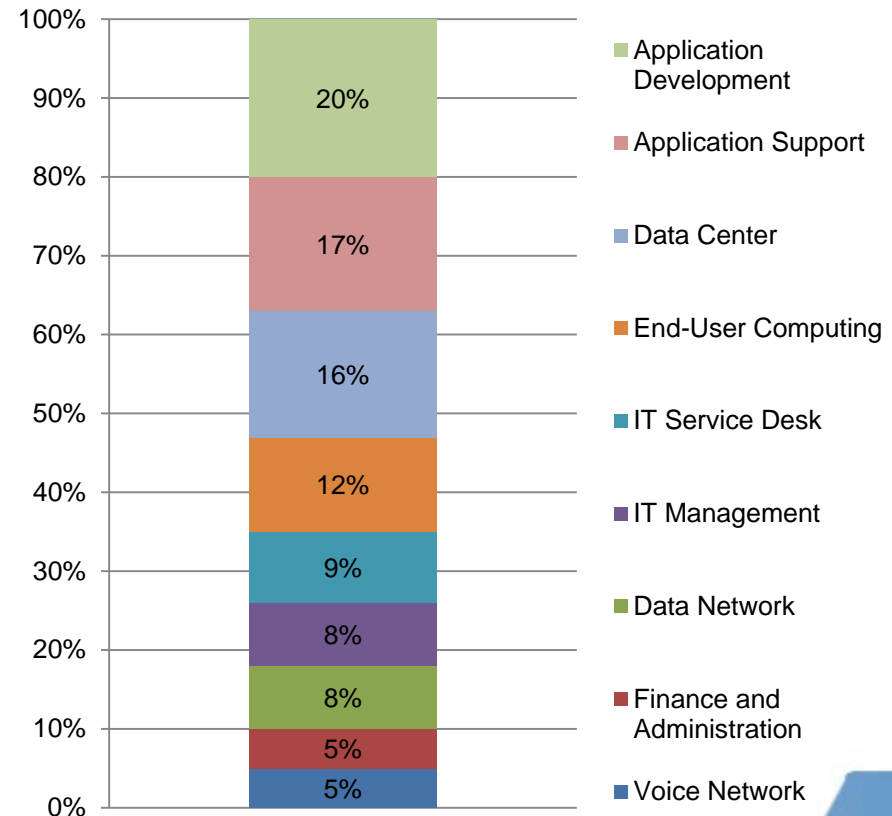NATIONAL INITIATIVE FOR **CYBER**SECURITY EDUCATION

U.S. IT Workforce Statistics

According to the U.S. Bureau of Labor Statistics, there are approximately 4.0 million people employed in the U.S. IT labor workforce.

Percentage of IT Workers by Sector

- **Private Sector** — 82%
- **Self-Employed** — 5%
- **Federal Gov't** — 4%
- 5%
- 3%

Percentage of IT Workers by Technology Domain

Technology Domain	Percentage
Application Development	20%
Application Support	17%
Data Center	16%
End-User Computing	12%
IT Service Desk	9%
IT Management	8%
Data Network	8%
Finance and Administration	5%
Voice Network	5%

*Source: CompTIA Colloquium 2012 - U.S. IT Market Supply and Demand Briefing

- **Mission Statement**

  "NICE will enhance the overall cybersecurity posture of the United States."

- **Goals**
  - Raise national awareness about risks in cyberspace
  - Broaden the pool of individuals prepared to enter the cybersecurity workforce
  - Cultivate a globally competitive cybersecurity workforce

Internal Component Structure

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NIST

C1	C2	C 3	C4
NATIONAL CYBERSECURITY AWARENESS	FORMAL CYBERSECURITY EDUCATION	CYBERSECURITY WORKFORCE STRUCTURE	CYBERSECURITY WORKFORCE TRAINING AND PROFESSIONAL DEVELOPMENT
DHS	**DoED NSF**	**DHS**	**DHS ODNI DOD**

NICE
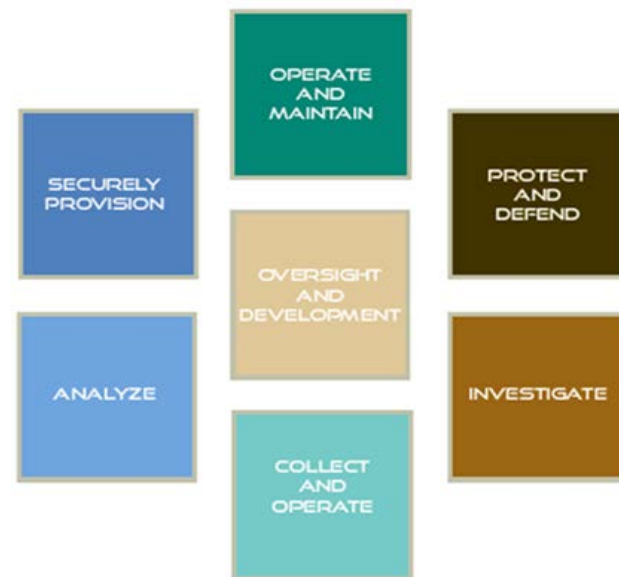NATIONAL INITIATIVE FOR **CYBER**SECURITY EDUCATION

A SOLUTION

NICE developed the National Cybersecurity Workforce Framework (the Framework) to codify cybersecurity work and to identify the specialty areas of cybersecurity professionals.

The Framework establishes:

- A common taxonomy and lexicon for cybersecurity workers that organizes cybersecurity into 31 specialty areas within 7 categories.
- A baseline of tasks, specialty areas, and knowledge, skills and abilities (KSAs) associated with cybersecurity professionals.

The Framework assists with strategic human capital efforts, including:

- Workforce planning
- Recruitment and Selection
- Training and Development
- Succession Planning

OPERATE AND MAINTAIN

SECURELY PROVISION

PROTECT AND DEFEND

OVERSIGHT AND DEVELOPMENT

ANALYZE

INVESTIGATE

COLLECT AND OPERATE

CYBERSECURITY WORKFORCE FRAMEWORK

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

National Cybersecurity Workforce Framework

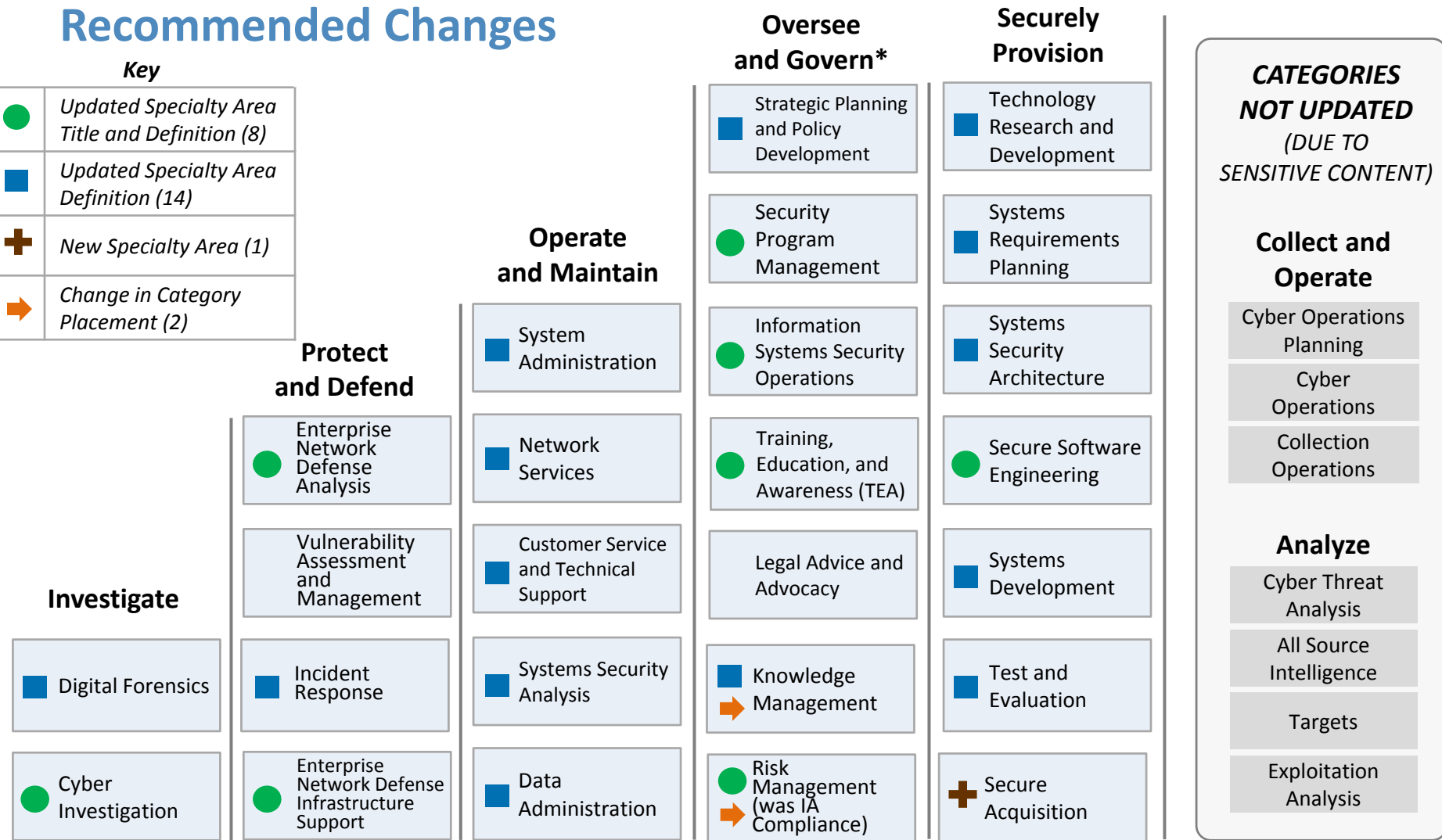|	
Securely Provision	**Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems, i.e., responsible for some aspect of systems development.**
Operate and Maintain	**Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.**
Protect and Defend	**Specialty area responsible for identification, analysis and mitigation of threats to internal information technology (IT) systems and networks.**
Investigate	**Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.**
Operate and Collect	**Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.**
Analyze	**Specialty area responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.**
Oversight and Development	**Specialty areas that providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.**

NICE
NATIONAL INITIATIVE FOR **CYBER**SECURITY EDUCATION

National Cybersecurity Workforce Framework

NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK v1.0*							
Categories	**Specialty Areas**						
Securely Provision	Information Assurance (IA) Compliance	Software Assurance and Security Engineering	Systems Security Architecture	Technology Research and Development	Systems Requirements Planning	Test and Evaluation	Systems Development
Operate and Maintain	Data Administration	Knowledge Management	Customer Service and Technical Support	Network Services	System Administration	Systems Security Analysis	
Protect and Defend	Computer Network Defense (CND) Analysis	Incident Response	Computer Network Defense (CND) Infrastructure Support	Vulnerability Assessment and Management			
Investigate	Digital Forensics	Investigation					
Collect and Operate	Collection Operations	Cyber Operations Planning	Cyber Operations				
Analyze	Threat Analysis	Exploitation Analysis	All Source Intelligence	Targets			
Oversight and Development	Legal Advice and Advocacy	Strategic Planning and Policy Development	Education and Training	Information Systems Security Operations (Information Systems Security Officer [ISSO])	Security Program Management (Chief Information Security Officer [CISO])		

*The Framework consists of thirty-one specialty areas organized into seven categories. These categories, serving as an overarching structure for the Framework, group related specialty areas together. In essence, specialty areas in a given category are typically more similar to one another than to specialty areas in other categories. Within each specialty area, typical tasks and knowledges, skills, and abilities (KSAs) are provided. The entire Framework is available at http://csrc.nist.gov/nice/framework/ .

Framework 2.0 Categories and Specialty Areas – Recommended Changes

Key

🟢	*Updated Specialty Area Title and Definition (8)*
🟦	*Updated Specialty Area Definition (14)*
➕	*New Specialty Area (1)*
➡️	*Change in Category Placement (2)*

Investigate

- 🟦 Digital Forensics
- 🟢 Cyber Investigation

Protect and Defend

- 🟢 Enterprise Network Defense Analysis
- 🟦 Vulnerability Assessment and Management
- 🟦 Incident Response
- 🟢 Enterprise Network Defense Infrastructure Support

Operate and Maintain

- 🟦 System Administration
- 🟦 Network Services
- 🟦 Customer Service and Technical Support
- 🟦 Systems Security Analysis
- 🟦 Data Administration

Oversee and Govern*

- 🟦 Strategic Planning and Policy Development
- 🟢 Security Program Management
- 🟢 Information Systems Security Operations
- 🟢 Training, Education, and Awareness (TEA)
- Legal Advice and Advocacy
- 🟦 ➡️ Knowledge Management
- 🟢 ➡️ Risk Management (was IA Compliance)

Securely Provision

- 🟦 Technology Research and Development
- 🟦 Systems Requirements Planning
- 🟦 Systems Security Architecture
- 🟢 Secure Software Engineering
- Systems Development
- 🟦 Test and Evaluation
- ➕ Secure Acquisition

CATEGORIES NOT UPDATED *(DUE TO SENSITIVE CONTENT)*

Collect and Operate

- Cyber Operations Planning
- Cyber Operations
- Collection Operations

Analyze

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

* The "Oversight and Development" Category name changes to "Oversee & Govern."

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

10

HOW THE FRAMEWORK
IMPACTS ALL FOUNDATIONAL ACTIVITIES

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

- *Key Activities*: Version 1.0 Released (Aug 2012), LRM Process (Dec 2012 – Mar 2013), OPM Data Element Guidance (Oct 2012), Framework How-To Implementation Guide (Dec 2012), Framework Roll-out (Ongoing)*

Training Catalog / NICCS: An online web resource with a robust collection of trainings mapped to the Framework.

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

IT Workforce Assessment: Collect data to identify the current state of the information technology workforce, and to assess current cybersecurity capabilities.

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

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

- *Key Activities*: Workforce Current Training Needs Report (Mar 2013), Training Gap Analysis Report (Jun 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 NICCS (2013)*

NICE

| National Cybersecurity Awareness | Formal Cybersecurity Education | **Cybersecurity Workforce Structure** | **Cybersecurity Professional Development** |
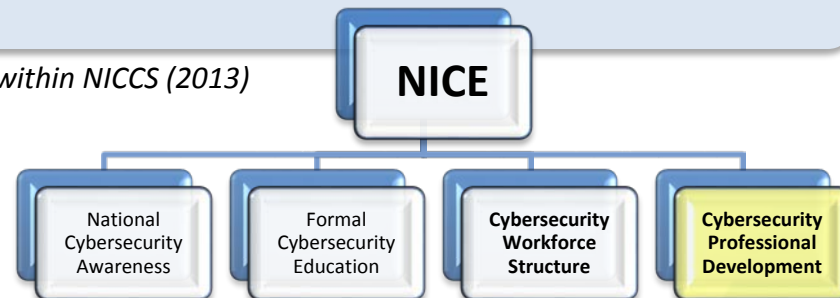
NICE
NATIONAL INITIATIVE FOR **CYBERSECURITY EDUCATION**

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

THE NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (NICCS) PORTAL

Serves as the Nation's online resource for cybersecurity awareness, education, careers, training, and professional development.

- Builds an online portal for cybersecurity professionals and interested parties to gain knowledge related to their field.

- Raises cybersecurity awareness and will affect a change in the American public to adopt a culture of cyberspace security.

- Provides up-to-date material related to cybersecurity awareness, education, careers, and training programs.

www.niccs.us-cert.gov

NEXT STEPS

Your assistance is critical to defining and creating a high-performing cybersecurity workforce. Next steps include:

- Exploring the NICCS website and learning how your organization can become involved.

- Becoming familiar with the Framework and its significance in human capital planning.

- Identifying points of contact (POCs) and champions in your organization to identify how to best adopt the Framework.

- Using the following How-To Guide to decide how to tailor the Framework to your your organization's workforce needs.

- Establishing an internal plan for adopting the Framework.

- Communicating the Framework with your network of colleagues.

- Linking implementation of the Framework to the Closing the Skills Gap effort.

- Developing Framework Version 2.0 began on June 21st, 2013, continues draft due due summer of 2014.

- NICE 2.0 on the way, transition to be completed by end of FY14.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

- Raised awareness about the risks of online activities

- Effective communication resources

- Annual NICE Workshop

- Activities focused on closing identified cybersecurity education, training, and awareness gaps

- Established metrics to measure progress

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

- Ernest McDuffie PhD
  - ernest.mcduffie@nist.gov
- [NICE Staff](#)
  - nice.nist@nist.gov
- [Website](#)
  - http://nist.gov/nice

NICE
NATIONAL INITIATIVE FOR **CYBER**SECURITY EDUCATION

WHITE HOUSE DEFINITION OF CYBERSECURITY

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

FRAMEWORK CATEGORIES AND SPECIALTY AREAS

*The Framework organizes cybersecurity work into 31 specialty areas within 7 categories. Each specialty area represents an area of concentrated work, or function, within cybersecurity. Below are the 7 categories (**bold**), with corresponding specialty areas.*

Securely Provision
Systems Requirements Planning
Systems Development
Software Assurance and Security Engineering
Systems Security Architecture
Test and Evaluation
Technology Research and Development
Information Assurance (IA) Compliance

Operate and Maintain
System Administration
Network Services
Systems Security Analysis
Customer Service and Technical Support
Data Administration
Knowledge Management

Collect and Operate
Collection Operations
Cyber Operations Planning
Cyber Operations

Protect and Defend
Vulnerability Assessment and Management
Incident Response
Computer Network Defense (CND) Analysis
Computer Network Defense (CND) Infrastructure Support

Investigate
Investigation
Digital Forensics

Analyze
Cyber Threat Analysis
Exploitation Analysis
Targets
All Source Intelligence

Oversight and Development
Legal Advice and Advocacy
Education and Training
Strategic Planning and Policy Development
Information Systems Security Operations (ISSO)
Security Program Management (Chief Information Security Officer [CISO])

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION