NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

What the roll-out of the National Cybersecurity Workforce Framework means to you!

Margaret “Peggy” Maxson and Dr. Michael Koehler
DHS Cybersecurity Education Office (CEO)

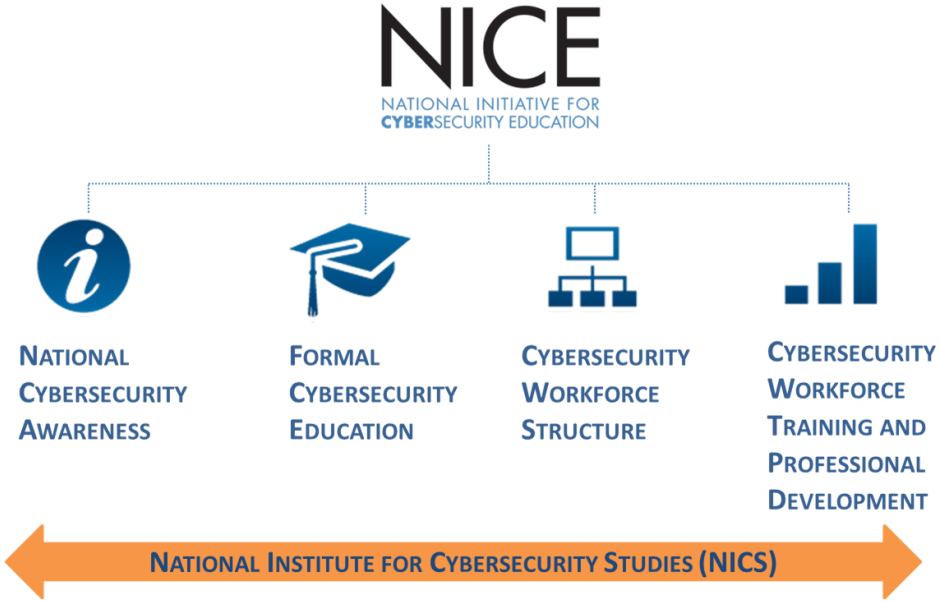
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Table of Contents

A National Problem

- The Nation needs greater cybersecurity awareness and more cybersecurity experts.
- There is a lack of communication among 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.

The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort created following the recognition in two Presidential directives of the need for a robust, competent cybersecurity workforce.



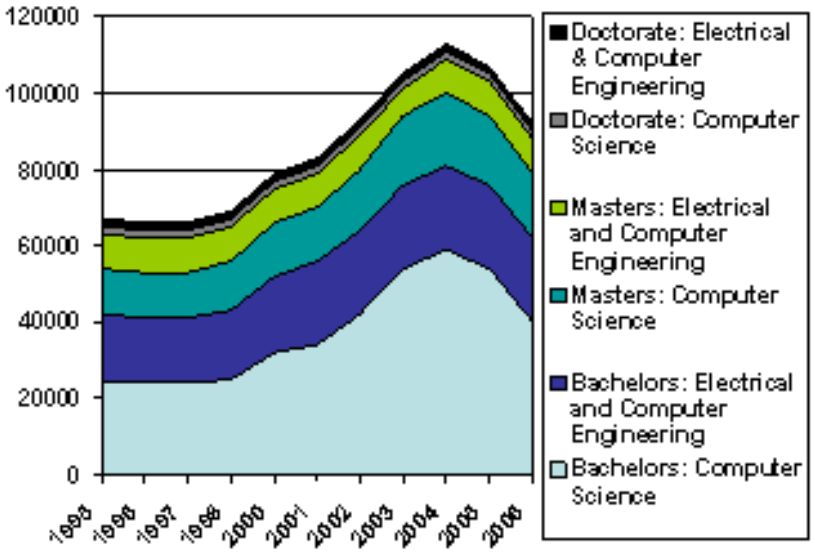
For more information on NICE, visit www.nist.gov/nice.

The Challenge

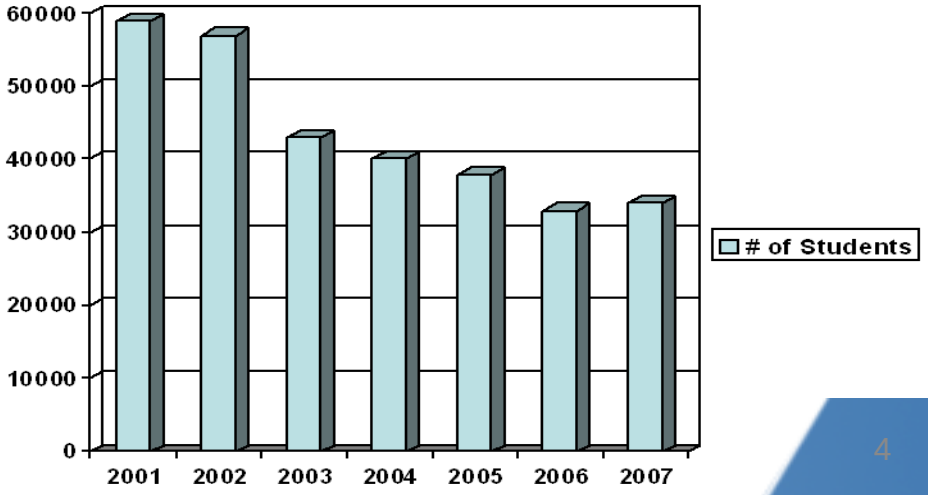
***TIMSS* Mathematics Test Score Comparison (2007): Avg. = 500 Source: *TIMSS* (2007)**

Grade	Four		Grade	Eight
Country	Score		Country	Score
Hong Kong	607		Chinese Taipei	598
Singapore	599		Rep. of Korea	597
Chinese Taipei	576		Singapore	593
Japan	568		Hong Kong	572
Kazakhstan	549		Japan	570
Russian Federat.	544		Hungary	517
England	541		England	513
Latvia	537		Russian Federat.	512
Netherlands	535		**United States**	**508**
Lithuania	530		Lithuania	506
United States	**529**		Czech Republic	504

Supply of Traditional NIT Graduates (1995-2000) (NCES)

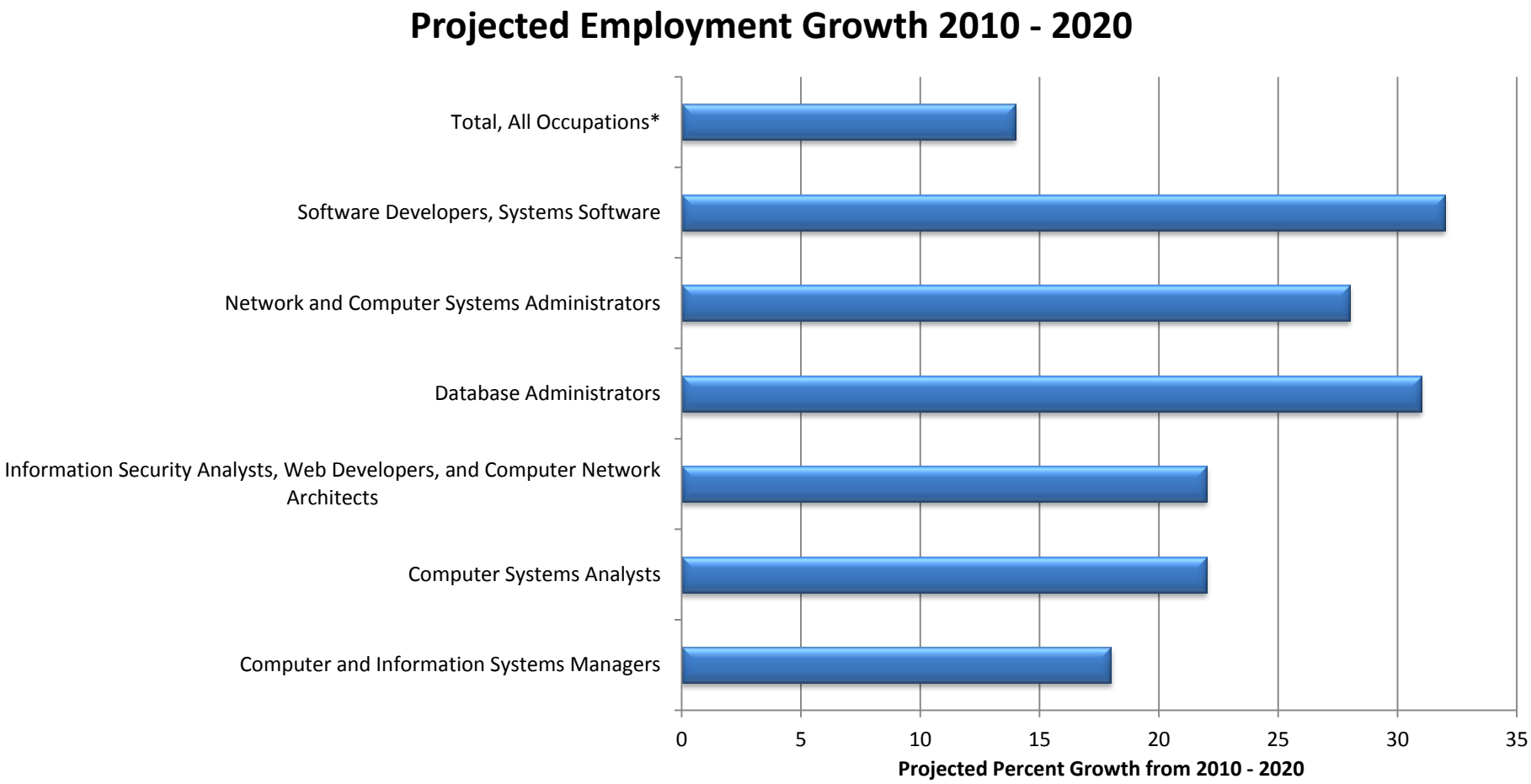


Computing and Information Sciences as Intended Major on SAT



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Employment Growth in Computer & IT Occupations

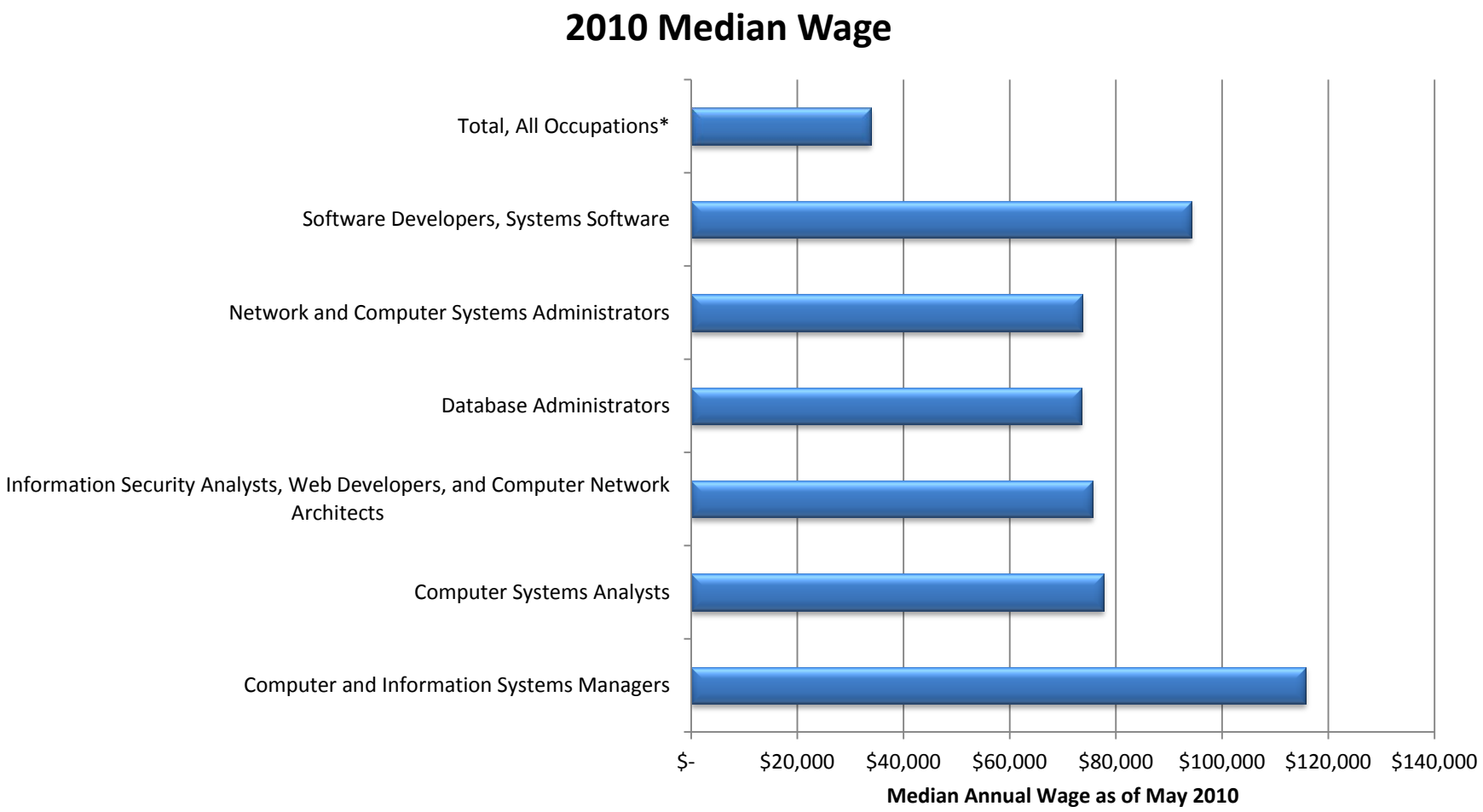


*All Occupations includes all occupations in the U.S. Economy.

Source: U.S. Bureau of Labor Statistics, Employment Projections Program

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Median Wages for Computer & IT Occupations

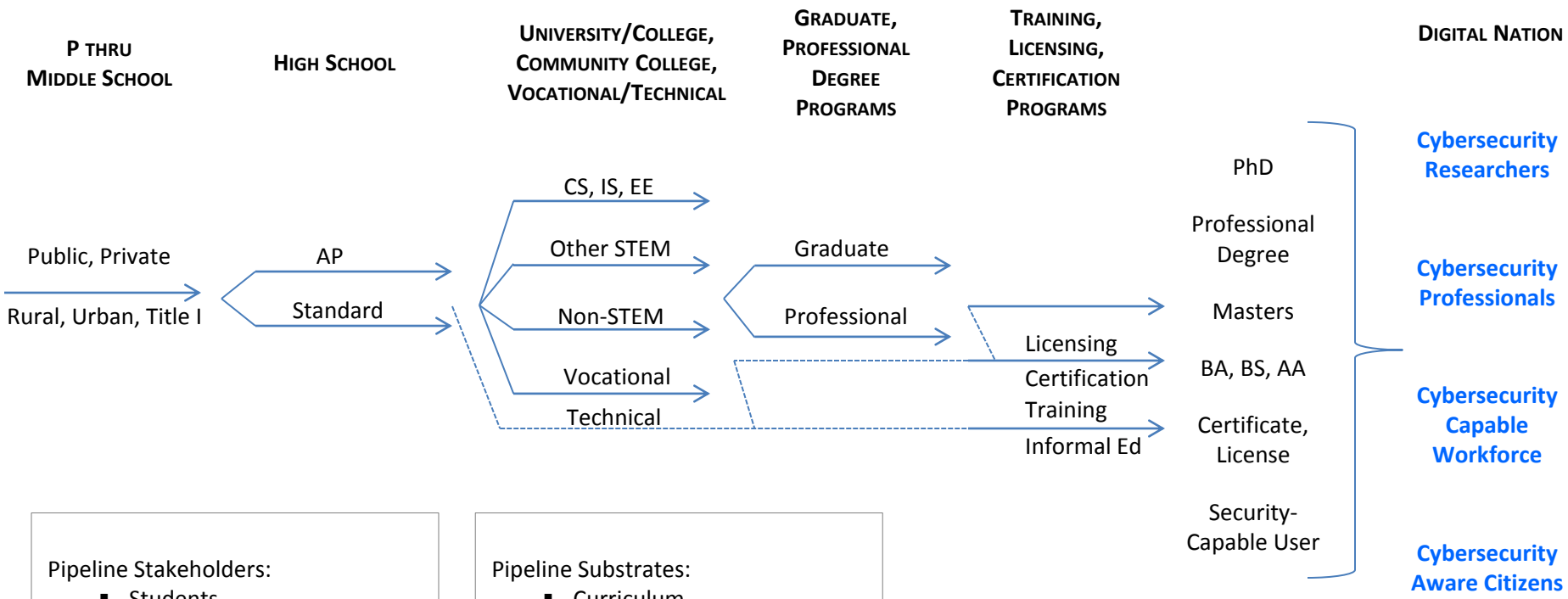


* All Occupations includes all occupations in the U.S. Economy.

Source: U.S. Bureau of Labor Statistics, Employment Projections Program

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The Pipeline



Pipeline Stakeholders:

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

Pipeline Substrates:

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

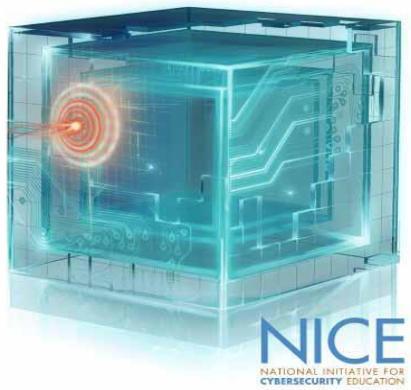
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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

Table of Contents



National Cybersecurity Workforce Framework

The Framework, 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.
- Find the framework @ http://www.nist.gov/nice/framework/

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.

NICE Workforce Training & Professional Development Timeline

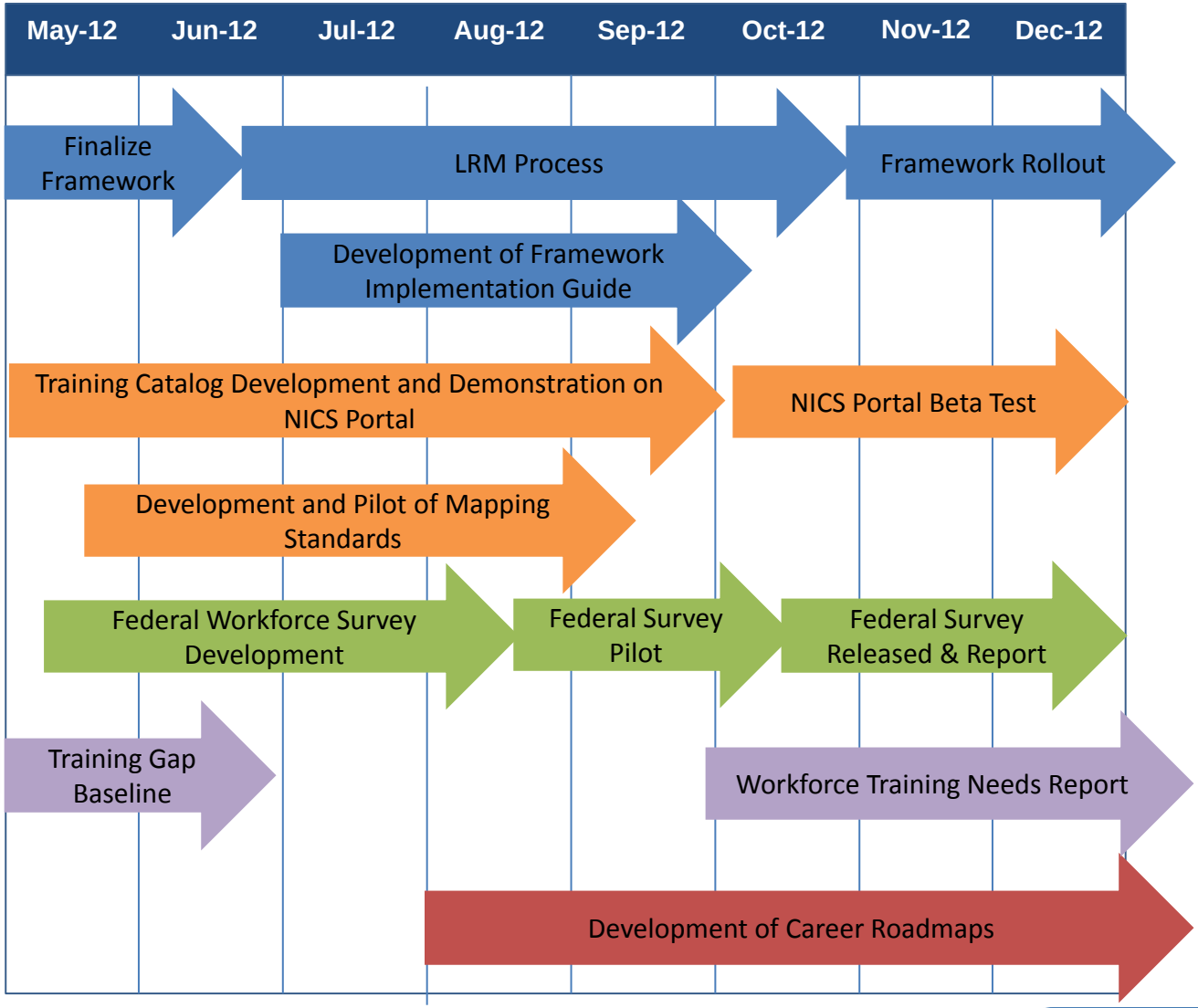
The Framework: Provides a common language to define cybersecurity work. The Framework defines specialty areas, KSAs, and competencies.

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

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

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

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



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Table of Contents

Cyber Workforce Inventory Program (CWIP)

A program made up of three projects with the goal of assessing the capabilities of the Nation's cybersecurity workforce using the Framework as a foundation.

Federal IT Workforce

- The NICE/CIO Council IT Workforce Assessment for Cybersecurity (ITWAC)

Non-Federal Workforce

- State, Local, Tribal, and Territorial governments, Academia, and Industry

Individuals

- Planned functionality through the NICS Portal to allow individuals to assess their cybersecurity competencies based on the Framework

Framework Implementation: Federal IT Workforce

Objective: Understand the composition and capabilities of the Federal IT workforce executing cybersecurity responsibilities.

- A government-wide survey of the workforce collecting self-assessments of individual cybersecurity competencies based on the Specialty Areas of the Framework.
- Implementation of this assessment will drive the acceptance and institutionalization of the Framework as the primary basis for Federal cybersecurity workforce organization, recruitment, and evaluation.

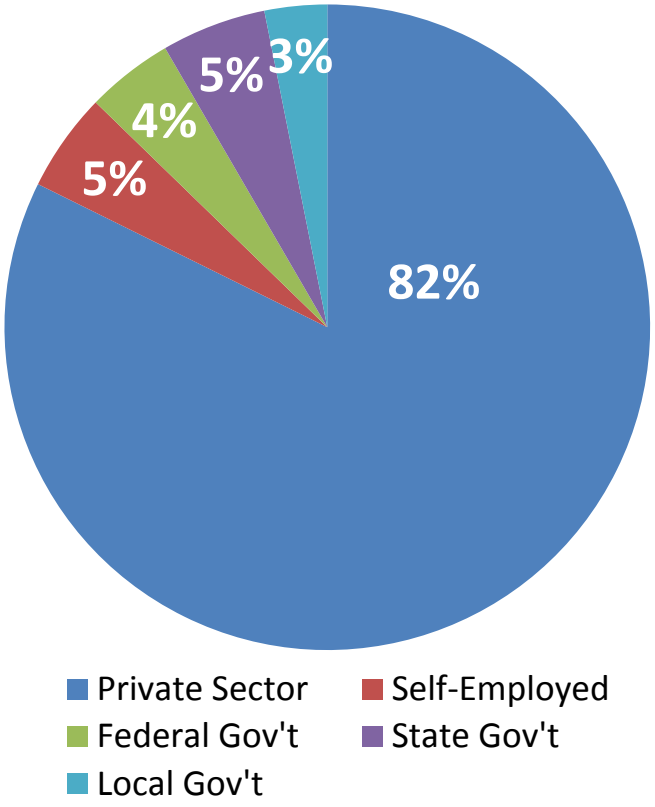
Implementation Impact

- Additional planned assessment activities include collecting data characterizing the Framework-based cybersecurity competencies of the Nation's IT workforce.
- The Framework will soon define the cybersecurity competencies of 80,000+ Federal IT professionals.
- The Framework can be used to establish competency expectations for private sector contract employees.
- As government-wide adoption of the Framework proceeds, expectations for a clear association between the Framework and cybersecurity education and training will grow.

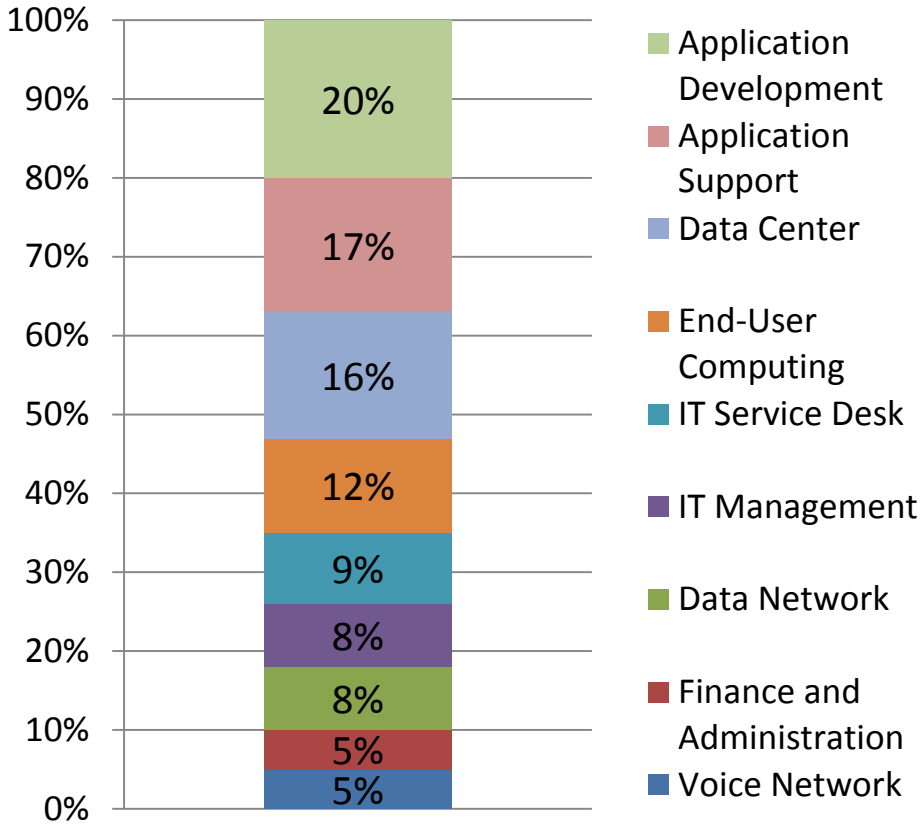
U.S. IT Workforce Statistics

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



Percentage of IT Workers by Technology Domain



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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

Summary

The National Cybersecurity Workforce Framework is being used by industry, academia, and government to:

- Inform students of available cybersecurity careers.
- Identify the need for education and training development.
- Describe the current cybersecurity workforce.
- Plan for the future cybersecurity workforce.

How can you use the Framework in your organization?

Contact Information

Peggy Maxson Margaret.Maxson@hq.dhs.gov

Dr. Michael Koehler Michael.Koehler@hq.dhs.gov

Find the framework @ http://www.nist.gov/nice/framework/