NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

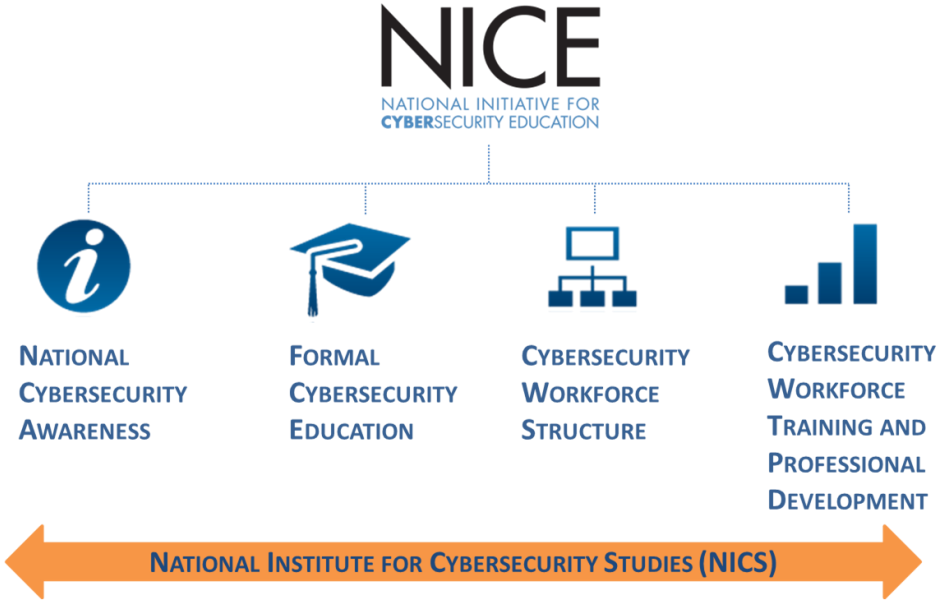
Component 3: Professionalizing the Cybersecurity Workforce

Angela Curry
National Cybersecurity Workforce Structure Strategy

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.

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.

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

COMPONENT 3: WORKFORCE STRUCTURE

It is the Workforce Structure component of NICE and focuses on the talent management of cybersecurity professionals.

Three complimentary focus areas:

- Professionalization - Component 3 will study the application of professionalizing certain specialty areas within the NICE framework.

- Workforce Planning - Component 3 aims to deliver a methodology for accurately forecasting cybersecurity workforces to help organizations better predict future cybersecurity needs. Determining your **supply** and **demand**.

- Recruitment and Retention - Component 3 intends to analyze the recruitment and retention strategies of other career fields in order to provide a best practice resource to help other organizations recruit and retain cybersecurity professionals.

PROFESSIONALIZATION –DEFINITION

The Fontana Dictionary of Modern Thought defines professionalization as, "when 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."

PROFESSIONALIZATION OBJECTIVES

Objective 1	• Research potential professionalization processes, and the impacts of each, by examining the history and procedures of occupations which have professionalized
Objective 2	• Analyze need for professionalizing cybersecurity workforce, and, if professionalization is deemed necessary, evaluate which of the 31 cybersecurity specialty areas will be professionalized
Objective 3	• Provide a set of governance standards for professionalization
Objective 4	• Socialize Professionalization implementation plan with Federal, State, Local, Tribal and Territorial governments and industry

PROFESSIONALIZATION – OBJECTIVE 1

Research potential professionalization processes, and the impacts of each, by examining the history and procedures of occupations which have professionalized

- *Examine historical case studies of occupations which have evolved into an accepted profession*
- *Understand how other occupations have professionalized, and evaluate the impacts (to include legal and financial) of professionalizing the cybersecurity workforce*

Professionalization – Historical Analysis

NICE Component 3 team researched historic examples of other professions and how they became professionalized. The professions examined were:

Air Traffic Controller

Firefighter

Contract Specialist

Physician

	Education Requirements						Licensing/Certification Requirements		
Qualifications	**Associates Degree**	**Vocational School**	**Bachelor Degree**	**Masters Degree**	**Ph.D.**	**Medical School**	**National Board Exam**	**Certification**	**License**
	Core Medical Fields								
Registered Nurse (RN)	X		X	X					X
Physician			X						X
Pharmacist			X	X	X				X
Veterinarian			X				X		X
	Medical-Related Fields								
Physical Therapist			X	X			X		
Ultrasound Technician (Sonographer)	X	X							
Medical Supply Technician	X	X							
Emergency Medical Technician (EMT)/Paramedic	X	X					X		X

PROFESSIONALIZATION – OBJECTIVE 2

Analyze need for professionalizing cybersecurity workforce, and, if professionalization is deemed necessary, evaluate which of the 31 cybersecurity specialty areas will be professionalized

- Work with stakeholders to determine the merits of, and define a criteria for evaluating, the professionalization of cybersecurity specialties based on research findings
- The evaluation of professionalization will include all stakeholders at a national level including Federal & State, Local, Tribal and Territorial (SLTT) governments, academic institutions, non-profits, and private industry through multiple public forums and other data gathering efforts. Transparency of this activity is not only critical, but a foundation of this project
- The public forums will be hosted by the National Academy of Science (NAS)

PROFESSIONALIZATION – OBJECTIVE 3

Provide a set of governance standards for professionalization

- *If a professionalization need is identified, the Component 3: Cybersecurity Professionalization Analysis project will build an implementation plan to institute a program and lay out policies and procedures for governing the professionalization of identified cybersecurity specialty areas*

PROFESSIONALIZATION – OBJECTIVE 4

Socialize Professionalization implementation plan with Federal, State, Local, Tribal and Territorial governments and industry.

- *If professionalization is deemed necessary, based on the NICE Strategic Plan:*
  - *Federal adoption for determining cybersecurity professionalization will occur by the end of 2013*
  - *Socialization among SLTT governments and industry by the end of 2015*

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

PROFESSIONALIZATION – SOCIALIZATION

Component 3 primarily engages with the Charter Group, a group of primary stakeholders expected to serve as trusted advisors. The Charter Group includes representatives from the following organizations:

- Department of Homeland Security (DHS)
- DHS National Cyber Security Division (DHS NCSD)
- Office of the Director of National Intelligence (ODNI)
- Department of Labor (DoL)
- Department of Education (DoE)
- Office of Personnel Management (OPM)
- National Institute of Standards and Technology (NIST)
- National Security Agency (NSA)
- State Department (State Dept.)
- Veteran's Affairs
- Department of Defense (DoD)
- U.S. Navy
- US CYBERCOM

Component 3 strives to collaborate with the rest of the Nation.

COMPONENT 3 MILESTONES &UPDATES

Milestones - *As of April 15, 2012*

- Component 3 established the Charter Group, comprised of 13 Federal departments and agencies.

Updates

- Workforce Planning – Component 3 has completed research into workforce planning best practices and processes. Research included looking at how organizations have already started to evaluate forecasting for cyber professionals and how cybersecurity changes the game, or what nuances should be taken into consideration for this field.

- Recruitment and Retention- Component 3 developed a cybersecurity professional profile through information collected from focus groups of individuals at all career levels and across all sectors (Federal, SLTT governments, industry, academia, non-profits, etc.). The information obtained will shape a national recruitment strategy and a national retention strategy for cybersecurity.

Contact Information

Angela Curry, Director, National Cybersecurity Workforce Strategy

Angela.Curry@dhs.gov

Chelsea Pickens, Component 3 Liaison

Chelsea_Pickens@sra.com

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