The attached document (provided here for historical purposes) has been superseded by the following:

Title: **National Initiative for Cybersecurity Education (NICE) Strategic Plan**

Date: **April 2016**

- The most recent NICE Strategic Plan can be found by visiting http://nist.gov/nice/about/
- More information about the National Initiative for Cybersecurity Education can be found by visiting http://nist.gov/nice/

NATIONAL INITIATIVE FOR **CYBER**SECURITY EDUCATION

STRATEGIC PLAN

NICE

NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

NIST NICE Component Leads

Overall Lead

Ernest L. McDuffie, Ph.D.
Lead for the National Initiative for Cybersecurity Education (NICE)
United States Department of Commerce (DoC)
National Institute of Standards and Technology (NIST)

Additional Leadership Support

R."Montana" Williams
Director
National Cybersecurity Education & Workforce Development Office
Department of Homeland Securit

Component 1 Lead

Kristina Dorville
Director, National Cybersecurity Education Strategy,
DHS

Component 2 Leads

Victor Piotrowski, Ph.D.
Lead Program Director (SFS)
Division of Undergraduate Education
National Science Foundation

John Manahan
U.S. Department of Education

Component 3 Lead

Angela Curry
Director, National Cybersecurity Workforce Structure Strategy
Department of Homeland Security

Support to Component 3

Sydney Smith-Heimbrock
Director Leadership and HR Development Solutions
OPM

Harold Welch
System Manager (Leadership and Knowledge Management), Agency and Program Review, Employee Services
OPM

Component 4 Leads

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

Jane Homeyer, Ph.D.
Deputy ADNI/Human Capital
Office of the Director of National Intelligence

John R. Mills
Special Assistant for Cybersecurity
DCIO Cybersecurity
DoD CIO
Office of the Secretary of Defense

Message from the Lead for the National Initiative for Cybersecurity Education

Our Nation's growing dependence on cyberspace is evident all around us. From smart phones and online banking to electronic health records, social networking, and automated manufacturing, our Nation increasingly relies on cyberspace. The scientists and innovators of tomorrow also rely on cyberspace to make the discoveries and inventions that improve our lives and drive our economy. The need for a safe and secure cyberspace has never been more important.

While there is no doubt that technology has changed the way we live, work, and play, there are very real threats associated with the increased use of technology and our growing dependence on cyberspace. For instance, cyber attacks on the Federal Government alone increased 680% from 2006 to 2011.[1] Also, the breach of the Sony PlayStation network in 2011 resulted in a leak of the private information of over 70 million customers.[2] Incidents like these reinforce the risks that exist in cyberspace and their potential impact in the real world.

Through education, the National Initiative for Cybersecurity Education (NICE) will counter these risks and help make cyberspace more secure. Education can prepare the general public to identify and avoid risks in cyberspace; education will ready the cybersecurity workforce of tomorrow; and education can keep today's cybersecurity professionals at the leading edge of the latest technology and mitigation strategies.

To address how education can help to ensure a more secure cyberspace, I am pleased to present to you the NICE Strategic Plan. This document outlines the goals of NICE as well as the objectives and strategies NICE will implement to achieve its goals. The partner agencies that comprise NICE are hard at work to address the Nation's cybersecurity education needs. Together, in partnership with our public and private stakeholders, NICE will make a difference in the future of cybersecurity in America.

Dr. Ernest McDuffie

Lead for the National Initiative for Cybersecurity Education (NICE)
United States Department of Commerce (DoC)
National Institute of Standards and Technology (NIST)

[1] http://www.executivegov.com/2012/04/gao-federal-cyberspace-incidents-up-680-over-5-years/
[2] http://news.cnet.com/8301-31021_3-20057577-260.html

Vision

A secure digital Nation capable of advancing America's economic prosperity and national security through innovative cybersecurity education, training, and awareness on a graduated scale that addresses the full spectrum of cybersecurity needs.

Mission

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

Goals

Table of Contents

Introduction

Released in 2009, the *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* acknowledged the need for cybersecurity public awareness and an advanced cybersecurity workforce. To address these needs, the Comprehensive National Cybersecurity Initiative (CNCI) developed 11 initiatives to help secure the United States in cyberspace. The National Initiative for Cybersecurity Education (NICE) was established to lead the work on the goals outlined in Initiative 8, which addresses the Nation's cybersecurity needs related to public awareness, education, professional development, and talent management.

CNCI Initiative 8:

Expand cyber education. While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge.

– Cyberspace Policy Review

In the past 20 years, the innovative use of cyberspace has transformed the day-to-day operations of the Nation. These advances have enhanced the lives of individuals, business, and government in profound ways. From eCommerce, to mobile communications and complex networked systems, the rapidly growing dependence on cyberspace is evident. In the years to come, the Nation's dependence on cyberspace will only increase as technology advances and will further integrate into our daily lives.

With great technological advances, however, come great risks. The Cyberspace Policy Review identified vulnerabilities in cybersecurity as systemic risks introduced into infrastructure, defense, and personal property due to the widespread adoption and dependence on technology. The more the Nation relies on cyberspace as a critical part of its infrastructure, the more responsibility there is to protect it. NICE will enhance the cybersecurity posture of the United States by achieving the following goals:

Goal 1. Raise national awareness about risks in cyberspace

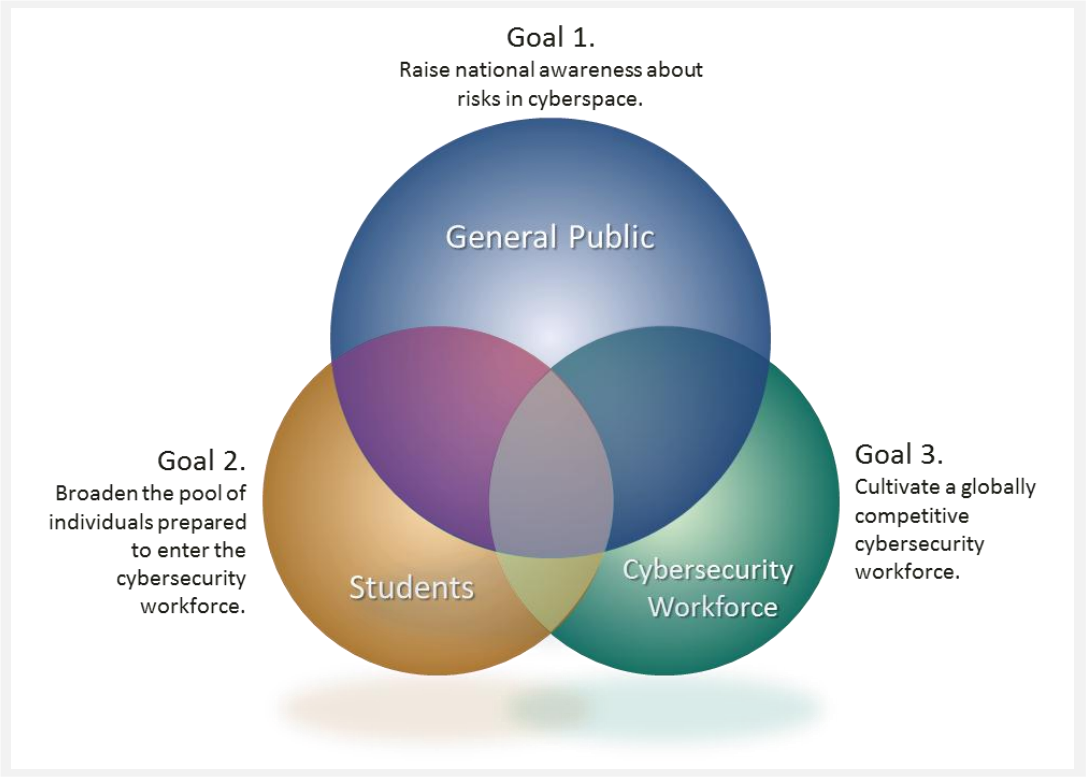
Goal 2. Broaden the pool of individuals prepared to enter the cybersecurity workforce

Goal 3. Cultivate a globally competitive cybersecurity workforce

Target Audience for NICE

Ensuring that the Nation is vigilant against the risks in cyberspace involves providing cybersecurity education to multiple segments of the population. These target audiences, depicted in Figure 1, include the general public, students, and the cybersecurity workforce.

Figure 1. Target Audience



The target audience for each goal is as follows:

Goal 1 focuses on the general public to provide basic information to both individuals and organizations on how to better protect themselves in cyberspace.

Goal 2 focuses on students at every level to increase interest in cybersecurity classes while better preparing students to pursue careers in cybersecurity.

Goal 3 focuses on the current cybersecurity workforce including providers, suppliers, and architects of cybersecurity to make the Nation's cybersecurity workforce the best in the world.

The education requirements for each audience correlate to the level of interaction and responsibility each group has in cyberspace. Because some people will interact with cyberspace on multiple levels and with

varying degrees of responsibility, there are overlaps in the target audiences, goals, and associated strategies. A more vigilant Nation in cyberspace will result from NICE's efforts to reach the target audiences.

Themes in the Strategic Plan

Stakeholders

Stakeholder support is central to the achievement of the NICE goals. Throughout this Strategic Plan, the term "stakeholders" represents a wide array of organizations that benefit from or work in partnership to achieve the NICE goals. Stakeholders generally include state, local, tribal, and territorial (SLTT) governments; non-profits; academic institutions; professional associations; community groups; and the private sector. NICE leverages partnerships with these stakeholders to attain each goal.

Each of the three goals described in this Strategic Plan has a key set of stakeholders. NICE initiates and maintains relationships with these stakeholders to best advance each goal. The relationship with stakeholders and the work they do in partnership with NICE is critical to the success of the goals of the overall initiative.

Consensus Building

Building consensus is one way to ensure ongoing success of an interagency initiative, where stakeholders each have independent, but complimentary, objectives. Throughout this Strategic Plan, NICE refers to "consensus building" when developing standards and guidelines for cybersecurity education. The method for developing standards and guidelines for NICE is a research and consensus-based approach that leverages the expertise of the NICE agencies. It is important to note that any standards, guidelines, tools, or other materials created by NICE are not presented as mandates, but are instead offered as guidance.

NICE Governance

NIST Role as NICE Lead

The National Institute of Standards and Technology (NIST) was appointed as the lead for NICE. In this role, NIST will support NICE in the following ways:

- Develop planning documents and build consensus on the strategy and implementation activities of NICE
- Facilitate cross-functional cooperation among NICE component lead agencies
- Foster communication between the component lead agencies by coordinating meetings, facilitating discussions, and disseminating information

- Promote the initiative and its efforts by representing NICE and speaking at cybersecurity events nationwide
- Plan and host an annual workshop to promote and support the evolving issues in cybersecurity education
- Coordinate with other Federal initiatives and efforts related to NICE
- Maintain and update the NICE Web site

Components

Currently, NICE is comprised of four components, depicted in Figure 2, each led by one or more Federal agencies. The efforts of Component 1 map to Goal 1 and are focused on raising awareness about the risks in cyberspace. Component 2 works to achieve Goal 2 through formal education partnerships to broaden the pool of individuals prepared to enter the cybersecurity workforce. Components 3 and 4 work to achieve Goal 3. Component 3 focuses on workforce planning, professionalization, and recruitment and retention in cybersecurity, while Component 4 targets the categorization, training, and development needs of the cybersecurity workforce. Together, Components 3 and 4 work to cultivate a globally competitive cybersecurity workforce. All components work cross-functionally and collaborate on projects to achieve the mission of NICE.

Figure 2. NICE Governance

A description of each component is as follows:

Component 1: National Cybersecurity Awareness. The lead agency for Component 1 is the Department of Homeland Security (DHS). The lead agency works with private, non-profit, and academic stakeholders to increase the public's understanding of cyber threats and empower the Nation to be safer and more secure online.

Component 2: Formal Cybersecurity Education. The co-lead agencies for Component 2 are the National Science Foundation (NSF) and the Department of Education (ED). The lead agencies work with educational associations, academia, and the Federal Government to develop the next generation

of cybersecurity workers by encouraging interest in science, technology, engineering, and mathematics (STEM) disciplines.

Component 3: Cybersecurity Workforce Structure. The lead agency for Component 3 is DHS. Component 3 involves collaboration with stakeholders across Federal departments and agencies, SLTT governments, industry, and academia to lay a foundation to evaluate the needs of and develop strategies for workforce planning, professionalization, recruitment, and retention for the cybersecurity field.

Component 4: Cybersecurity Workforce Training and Professional Development The co-lead agencies of Component 4 are DHS, the Department of Defense (DoD), and the Office of the Director of National Intelligence. Component 4 brings together government, industry, and academic stakeholders on the development and adoption of the National Cybersecurity Workforce Framework, as well as tools for measuring the current capabilities of the workforce, providing workforce training, and supporting professional development.

The four components work together on a continuous basis toward achieving the goals of NICE, and each has tactical plans and projects to help them execute strategies to attain each goal.

Success Indicators

Successful progress towards the NICE goals will be evident as the following actions occur:

- Online safety practices are understood, encouraged, and undertaken nationwide by both individuals and organizations of all disciplines and sizes.
- Cybersecurity positions are filled with qualified candidates.
- The National Cybersecurity Workforce Framework is referenced by the public and private sector when describing any information technology (IT) positions that require cybersecurity knowledge and abilities.

Strategic Planning

This Strategic Plan identifies goals, objectives, and strategies that will contribute to the realization of a more cyber-secure Nation and a globally competitive cybersecurity workforce. The goals provide guidance for executing NICE's mission and achieving its goals.

As the Nation progresses further into the 21st century, the risks in cyberspace are expected to grow based on the combination of two primary factors:

- A deeper reliance on cyberspace that allows for more cyber attack opportunities
- The rapid changes in technology that make staying ahead of cybersecurity risks a challenge

Because the cyberspace landscape and the way in which people access and use cyberspace are ever-changing, NICE will periodically evaluate and adjust its approach to ensure that it is addressing the most current needs in cybersecurity education. The following section of this Strategic Plan outlines the objectives and strategies for how NICE will achieve each of the three goals.

Goal 1. Raise National Awareness About Risks in Cyberspace

Individuals and organizations alike depend on cyberspace. From the casual consumer using social media, to online merchants growing their business, to physicians supporting their patients – every sector of our society is increasingly dependent upon technology and networked systems. Without sufficient awareness of the risks in cyberspace, however, behavioral decisions and unseen threats can negatively impact the security of the global cyberspace infrastructure and can cause physical damage in the real world. On an individual level, what is at stake is the vulnerability of each individual user in cyberspace. An individual who is not aware of, and does not implement, basic cybersecurity practices faces greater personal risk on and offline, such as identity theft, when engaging in daily online tasks.

NICE will work to improve the general public's knowledge of the risks in cyberspace and promote the use of cybersecurity resources and tools to reduce risk in the face of the Nation's increasing dependencies on cyberspace.

Objective 1.1 Improve Knowledge of Risks and Vulnerabilities in Cyberspace

Much of the general public may not be fully aware of the risks of operating in cyberspace, which can affect both personal and national security. All individuals who go online share responsibility for a more secure cyberspace and need to be aware of the risks and vulnerabilities in cyberspace. Protecting personal information and that of others, reinforcing their systems against attacks, and guarding against the use of their own systems in attacks, help individuals create a more secure cyberspace for everyone.

> The general public needs to be well informed to use the technology safely.
> *- Cyberspace Policy Review*

NICE will partner with stakeholders to build consensus around developing awareness messages and effective delivery mechanisms for sharing them. NICE will also leverage relationships with stakeholders to ensure that awareness messaging and materials are developed with academic rigor that can be tailored for multiple delivery methods, such as courses, competitions, and after-school programs.

The Stop.Think.Connect. campaign is designed to increase the awareness of the risks in cyberspace and to encourage individuals and organizations to change the behaviors that expose them to online risks. In addition to this campaign, NICE will also promote digital literacy training efforts to help individuals better understand the cybersecurity features on the devices they use.

Strategies

1. Promote cybersecurity awareness through campaigns such as Stop.Think.Connect.
2. Promote strategies for training the public to manage cyber risk

Objective 1.2 Promote the Use of Cybersecurity Resources and Tools

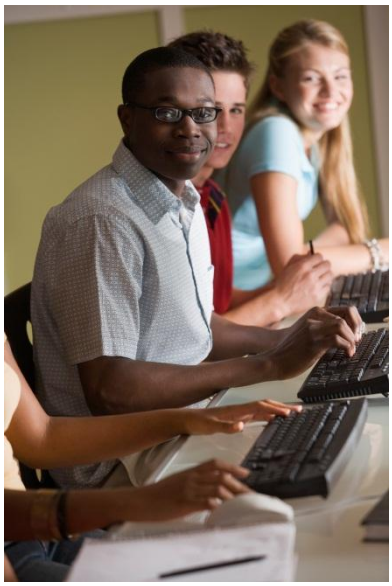
Oftentimes technology users are overwhelmed by the variety of cybersecurity tools and resources available to them, and do not know which tools to choose or which privacy or security settings to use to ensure their safety online. NICE will work to build consensus among cybersecurity experts and stakeholders to provide resources and tools that mitigate risks, can be effectively deployed, and are easy to use. Effective use of these cybersecurity resources will lower the risks in cyberspace for everyone and strengthen the cybersecurity infrastructure.

NICE will also encourage participation in activities that engage local communities and focus on a call to action to manage risks in cyberspace. Involvement in the cybersecurity community provides an opportunity for individuals and organizations to connect over shared cybersecurity needs and to share information, raise awareness levels, uncover resources, and ultimately build a more cyber-secure Nation. One way the Stop.Think.Connect. campaign and NICE are accomplishing this through “cyber tours.” A cyber tour brings together local academic institutions, government, non-profits, and community groups for a week of activities to promote cybersecurity awareness.

Strategies

1. Partner with external stakeholders
2. Encourage participation in cybersecurity-focused activities

Goal 2. Broaden the Pool of Individuals Prepared to Enter the Cybersecurity Workforce



As the world grows more connected through cyberspace, a highly skilled cybersecurity workforce is required to secure, protect, and defend our Nation's information systems. Across the Nation, private- and public-sector organizations are looking for well-trained professionals to assess, design, develop, and implement cybersecurity solutions and strategies. While the demand for cybersecurity professionals is high, the supply is low. Meeting the growing demand for cybersecurity professionals begins in the education system. NICE will work to increase the number of people emerging from the educational system with the skills necessary to meet the Nation's cybersecurity workforce needs. In concert with key stakeholders, NICE will stimulate early interest in cybersecurity by encouraging PreK-12 educators to emphasize connections between cybersecurity and the STEM skills our cybersecurity workforce needs. NICE will promote interest in pursuing courses fundamental to cybersecurity careers through a number of measures, and will work with key stakeholders to increase the quantity and diversity of computer science and computer engineering courses as well as research opportunities.

Objective 2.1 Increase Exposure to Cybersecurity in PreK-12 education by Emphasizing Connections to Science, Technology, Engineering, and Mathematics (STEM) Education and the Role of Mathematics and Computational Thinking in Cybersecurity

To remain globally competitive and secure in cyberspace, the Nation needs the next generation of cybersecurity workers to be problem-solvers and innovators who can think logically to tackle tomorrow's cybersecurity challenges. To address this need, educators and officials are working to develop evidence-based education standards that will support stronger STEM learning. NICE will encourage the fundamental concepts to cybersecurity to be incorporated into these new education standards to make students more aware of cybersecurity concepts and potential career opportunities.

> **Evidence-Based Education** is the integration of professional wisdom with the best empirical evidence in making decisions about how to deliver instruction.
> *- US Department of Education*

NICE will also partner with stakeholders to make the connection between STEM education and cybersecurity, and increase student exposure to cybersecurity themes. NICE wants to build cybersecurity into the real-life examples used by teachers in their math and science explorations.

> The United States should initiate a K-12 cybersecurity education program for digital safety, ethics, and security; expand university curricula; and set the conditions to create a competent workforce for the digital age.
> *- Cyberspace Policy Review*

Another objective in making the connection between STEM education and cybersecurity is to stress the importance of computational thinking in formal education. Computational thinking draws on the concepts that are fundamental to computer science and uses them to solve problems, design systems, and understand human behavior.[3] Computational thinking provides tools for how to approach complex tasks, systems, and problems, and, although it has many applications in other STEM fields, it is critical to cybersecurity.

Additionally, cybersecurity is a foundational underpinning of all STEM fields. Professionals in STEM-related fields often depend on cyberspace to conduct their work. It would be beneficial to all STEM professionals to understand the importance of cybersecurity in regards to their own work.

Great strides in STEM education are being made at all levels. NICE plans to leverage these efforts to promote interest in, and increase exposure to, cybersecurity by helping educators more clearly make the connection between STEM education and cybersecurity.

Strategies

1. Disseminate common evidence standards in PreK-12 education
2. Incorporate cybersecurity into Federal PreK-12 STEM efforts
3. Encourage partnerships with stakeholders to enhance PreK-12 cybersecurity education

Objective 2.2 Promote Interest in Computer Science and Cybersecurity by Increasing the Diversity and Quantity of Course Offerings and Research Opportunities

Without exposure to computer science and experience with computational challenges, students may not be introduced to, or prepared for, potential cybersecurity careers upon graduation. To increase the number and diversity of course offerings at the high school and collegiate level, NICE will facilitate the development of recommendations for computer science and cybersecurity curriculum. Improved course offerings that keep

[3] Wing, Jeannette M. "Computational Thinking". *Communications of the ACM*. March 2006. *49*(3), 33-35.

up with changing technology and the evolving threats in cyberspace will enhance student interest in potential careers in cybersecurity.

NICE will also support cybersecurity competitions. Competitions provide an interactive and hands-on approach to learning cybersecurity skills at all levels, and can be used as recruiting tools for potential employers. NICE will promote the development of cybersecurity training materials for high schools participating in competitions. NICE will also bring together competition organizers to work cooperatively to ensure that the cybersecurity skills needed by our Nation are incorporated into the competitions, while maximizing student opportunities to participate. As a relatively new field of study, cybersecurity has many areas that require further research and development. NICE will promote opportunities in research and development to encourage graduate students to consider cybersecurity as a focus for study, such as encouraging public and private scholarships and grant programs. This effort will also foster the development of professors capable of supporting future generations of cybersecurity students.

NICE will also coordinate among stakeholders to investigate the value and feasibility of developing cyber ranges, such as virtual cybersecurity laboratories, as a means to advance education and research in cybersecurity. Cyber ranges provide a realistic cyber attack environment for training and would promote collaboration and resource sharing among education institutions. Cyber ranges would also make remote learning and virtual cybersecurity modeling more accessible to students nationwide.

Strategies

1. Increase the quantity and diversity of computer science courses in high schools
2. Increase the quantity and diversity of undergraduate and graduate cybersecurity curricula
3. Champion cybersecurity competitions
4. Advance excellence in cybersecurity research and development
5. Coordinate a learning network of virtual national cybersecurity laboratories

Goal 3. Cultivate a Globally Competitive Cybersecurity Workforce

The talent and knowledge of the cybersecurity workforce is of significant concern across all business areas of the national landscape; however, the cybersecurity industry is still in its infancy and many aspects of this new industry are not yet defined. As the Nation defends against increasing threats in cyberspace, it is important to shape this emerging industry in a way that will maximize its impact in a safer cyberspace. Effective human capital planning is an identified need in the cybersecurity workforce and will enable the Nation to have the right people, with the right skills, at the right time and place. NICE will examine the current state of the cybersecurity workforce and provide guidance on human capital planning tools to ensure global competitiveness.

Through the achievement of Goal 3, NICE will lay the groundwork for building a robust and agile cybersecurity workforce. NICE will establish recommended standards and strategies for national cybersecurity training and career development, as well as methods for categorizing cybersecurity jobs and forecasting cybersecurity human capital needs. Additionally, NICE will analyze recruitment and retention strategies of other industries and evaluate the professionalization of the cybersecurity workforce.

Objective 3.1 Encourage the Development and Adoption of the National Cybersecurity Workforce Framework

As an emerging field, cybersecurity lacks common terminology for career maps, position descriptions, and knowledge, skills, and abilities. NICE has developed the National Cybersecurity Workforce Framework (the Framework) to address this need. The Framework provides a common language and taxonomy to characterize cybersecurity work, define specialty areas and competencies, and codify cybersecurity talent. The Framework is designed to be comprehensive and inherently flexible, allowing organizations to adapt its content to their own human capital and workforce planning needs. Because it is a living document, subject matter experts and key stakeholders will continue to discuss and validate the Framework.

Developing the Framework was the first step in providing a common lexicon for the cybersecurity workforce. The next step is the adoption of the Framework. NICE plans to monitor the adoption and provide tools to improve the adoption rate. In the fall of 2012, NICE intends to publish the Framework. The Office of

Personnel Management (OPM) has indicated that after the Framework is published, it will issue codes that correspond to the functional categories and specialty areas outlined in the document. The use of these codes will enable the OPM and Federal agencies to identify the cybersecurity workforce consistently across the Federal Government and determine a baseline of capabilities, examine workforce demands, identify training gaps, and more effectively recruit, hire, train, develop, and retain a world class cybersecurity workforce. NICE will also catalog and leverage the lessons learned from early adopters of the Framework to help pave the way for future adopters.

Strategies

1. Build consensus among key stakeholders to develop and validate the Framework
2. Develop tools that encourage and monitor the adoption of the Framework across all Federal agencies
3. Leverage lessons learned from adoption of the Framework to facilitate adoption in Federal, State, Local, Tribal, and Territorial governments and the private sector

Objective 3.2 Develop Cybersecurity Workforce Forecasting Tools

While there is an acknowledged need for more cybersecurity professionals, a consistent methodology for characterizing the size of the cybersecurity workforce does not exist. To know how to forecast Federal cybersecurity needs, a quantitative assessment of the Federal cybersecurity workforce is needed. NICE will support the collection of data to assess the current cybersecurity competencies of the Nation's IT workforce in accordance with the lexicon in the Framework. This data will create a baseline of understanding of the characteristics of the Nation's cybersecurity workforce that could be used for future planning across multiple sectors.

Once a baseline is established, NICE will support the research and development methods for forecasting future needs. Research will include an examination of how organizations in various industries currently forecast workforce needs and how the unique challenges of a given industry might affect forecasting.

Strategies

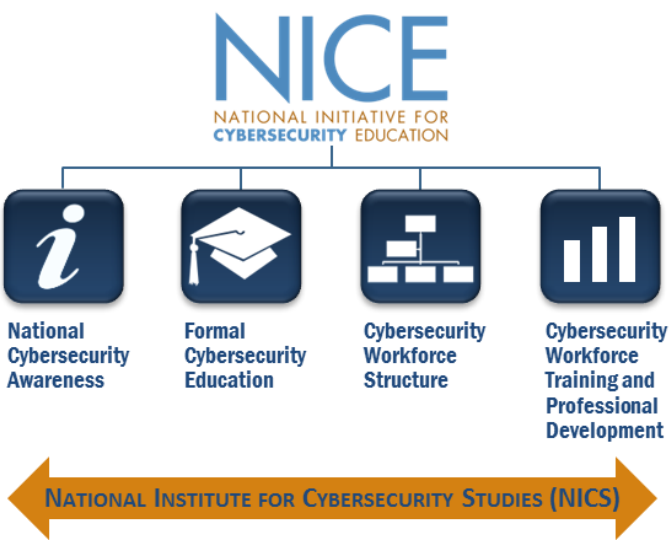
1. Assess the Federal cybersecurity workforce, utilizing the guidance in the Framework
2. Research and identify best practices for forecasting cybersecurity needs

Objective 3.3 Establish Standards and Guidance for Cybersecurity Training and Professional Development

A world class cybersecurity workforce will require ongoing, specialized training. Specialized cybersecurity training ensures that the cybersecurity workforce has the technical skills, resources, and credibility to fulfill its role. As requirements of the cybersecurity workforce evolve, an online database of cybersecurity training information will help to establish training efforts that are targeted to meet changing needs. The National Institute for Cybersecurity Studies (NICS) portal, depiced in Figure 3, will be an online resource designed to improve cybersecurity workforce training by providing a robust and representative resource of available cybersecurity training opportunities that align to the specialty areas within the Framework.

Cybersecurity professionals need a clear path for professional development that not only promotes individual advancement, but also helps fill cybersecurity positions with individuals who have the knowledge, skills, and abilities needed. Using the Framework as a guide, NICE plans to develop materials that clearly illustrate how to acquire or improve the knowledge and skills necessary for advancement in cybersecurity positions. Career maps that depict progression from entry to expert will guide individuals through requisite training for a career in cybersecurity.

Figure 3. NICS Portal



The gaps between currently available training opportunities for the Federal cybersecurity workforce and the specialty areas represented throughout the Framework are currently unknown. Gaps in training create risks to the Nation's cybersecurity readiness. NICE will coordinate a gap analysis to help mitigate those risks and develop a training catalog for the Federal cybersecurity workforce that addresses any gaps identified.

Strategies

1. Develop a baseline of current cybersecurity training opportunities
2. Utilize the Framework to classify training programs based on proficiency, career level, and specialty area
3. Provide guidelines detailing how to acquire or improve the knowledge and skills necessary for cybersecurity positions outlined in the Framework

4. Develop tools, such as the National Institute for Cybersecurity Studies (NICS) Portal, to provide access to a catalog of training and courses that map to the Framework
5. Identify and mitigate gaps in cybersecurity training

Objective 3.4 Analyze and Identify Best Practices to Help Organizations Recruit and Retain Cybersecurity Professionals

Both the public and private sectors have difficulty retaining high performing employees in cybersecurity roles. NICE will examine best practices for recruitment and retention to provide tools and strategies to help employers retain valuable cybersecurity personnel.

Strategies

1. Analyze recruitment and retention strategies of other career fields
2. Provide best practice resources to help organizations recruit and retain cybersecurity professionals

Objective 3.5 Evaluate the Professionalization of the Cybersecurity Workforce

The cybersecurity industry is a relatively new industry. By looking at more mature professions, such as medicine and air traffic control, NICE will examine possible paths to professionalization for the cybersecurity workforce. By understanding the options and potential impacts of professionalization in other industries, NICE will help to define the role of professionalization in the cybersecurity industry.

Strategies

1. Research the professionalization processes in other occupations and the impact on the field
2. Characterize the potential impacts of professionalizing the cybersecurity workforce

Appendix

Appendix A. Goals, Objectives, Strategies

Goal	Objective	Strategy
1. Raise national awareness about risks in cyberspace	1.1 Improve knowledge of risks and vulnerabilities in cyberspace	1. Promote cybersecurity awareness through campaigns such as Stop.Think.Connect.
		2. Promote strategies for training the public to manage cyber risk
	1.2 Promote the use of cybersecurity resources and tools	1. Partner with external stakeholders
		2. Encourage participation in cybersecurity-focused activities
2. Broaden the pool of individuals prepared to enter the cybersecurity workforce	2.1 Increase exposure to cybersecurity in PreK-12 education by emphasizing connections to Science, Technology, Engineering, and Mathematics (STEM) education and the role of mathematics and computational thinking in cybersecurity	1. Disseminate common evidence standards in PreK-12 education
		2. Incorporate cybersecurity into Federal PreK-12 STEM efforts
		3. Encourage partnerships with stakeholders to enhance PreK-12 cybersecurity education
	2.2 Promote interest in computer science and cybersecurity by increasing the diversity and quantity of course offerings and research opportunities	1. Increase the quantity and diversity of computer science courses in high schools
		2. Increase the quantity and diversity of undergraduate and graduate cybersecurity curricula
		3. Champion cybersecurity competitions
		4. Advance excellence in cybersecurity research and development
		5. Coordinate a learning network of virtual national cybersecurity laboratories
3. Cultivate a globally competitive cybersecurity workforce	3.1 Encourage the development and adoption of the National Cybersecurity Workforce Framework	1. Build consensus among key stakeholders to develop and validate the Framework
		2. Develop tools that encourage and monitor the adoption of the Framework across all Federal agencies
		3. Leverage lessons learned from adoption of the Framework to facilitate adoption in Federal, State, Local, Tribal, and Territorial governments and the private sector

Goal	Objective	Strategy
3. Cultivate a globally competitive cybersecurity workforce (Re-stated)	3.2 Develop cybersecurity workforce forecasting tools	1. Assess the Federal cybersecurity workforce, utilizing the guidance in the Framework
		2. Research and identify best practices for forecasting cybersecurity needs
	3.3 Establish standards and guidance for cybersecurity training and professional development	1. Develop a baseline of current cybersecurity training opportunities
		2. Utilize the Framework to classify training programs based on proficiency, career level, and specialty area
		3. Provide guidelines detailing how to acquire or improve the knowledge and skills necessary for cybersecurity positions outlined in the Framework
		4. Develop tools, such as the National Institute for Cybersecurity Studies (NICS) portal, to provide access to a catalog of training and courses that map to the Framework
		5. Identify and mitigate gaps in cybersecurity training
	3.4 Analyze and identify best practices to help organizations recruit and retain cybersecurity professionals	1. Analyze recruitment and retention strategies of other career fields
		2. Provide best practice resources to help organizations recruit and retain cybersecurity professionals
	3.5 Evaluate the professionalization of the cybersecurity workforce	1. Research the professionalization processes in other occupations and the impact on the field
		2. Characterize the potential impacts of professionalizing the cybersecurity workforce

Appendix B. Partner Agencies

Partner	Description
Department of Commerce – NIST	Founded in 1901, the National Institute of Standards and Technology (NIST) is a non-regulatory Federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. www.nist.gov NIST acts as the coordinating agency for NICE.
Department of Defense	Established in 1789, the Department of Defense (DoD) is America's oldest and largest government agency. The mission of DoD is to provide the military forces needed to deter war and to protect the security of our country. www.defense.gov DoD is a co-lead for Component 4 of NICE.
Department of Education	The Department of Education (ED) was created in 1980 by combining offices from several Federal agencies. ED's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access. www.ed.gov ED is a co-lead for Component 2 of NICE.
Department of Homeland Security	The Department of Homeland Security (DHS) combined 22 different Federal departments and agencies into a unified, integrated cabinet agency when it was established in 2002. DHS has a vital mission: to secure the Nation from the many threats we face. www.dhs.gov DHS is co-lead on Components 1, 3, and 4 of NICE.
National Science Foundation	The National Science Foundation (NSF) is an independent Federal agency created by Congress in 1950 to promote the progress of science; to advance the national health, prosperity, and welfare; and to secure the national defense. www.nsf.gov NSF is a co-lead for Component 2 of NICE.
Office of Personnel Management	Originally established as the United States Civil Service Commission in 1883, the Office of Personnel Management (OPM)'s mission is to recruit, retain, and honor a world-class workforce to serve the American people. www.opm.gov OPM is a co-lead for Component 3 of NICE.

Appendix C. Glossary

Term	Description
Cyber range	Provides a unique testing environment that allows large and small scale networks to be simulated using a mixture of virtual and physical devices.
Cybersecurity	The strategy, policy, and standards regarding the security of and operations in cyberspace; 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	The interdependent network of IT infrastructures, which includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.
Cyber Tours	A cyber tour spends a week in a community and brings together local academic institutions, government, non- profits, and community groups to promote cybersecurity awareness.
Education System	The teaching bodies (educators, students, and institutions) and academic mechanisms (curricula, resources, training, awards, and competitions) that comprise formal education in the Nation.
Evidence Based Education	The integration of professional wisdom with the best empirical evidence in making decisions about how to deliver instruction.
National Cybersecurity Workforce Framework (the Framework)	The Framework provides a baseline of knowledge, skills, and abilities for professionals across the diverse array of cybersecurity disciplines, and a foundation for the education and training necessary to excel in these careers; facilitates the identification of training needs; and guides the design of a professional development program.
SLTT	Federal acronym for state, local, tribal, and territorial, which refers to those non-Federal Governments.
Stakeholders	Generally includes SLTT governments, non-profits, academic institutions, professional associations, community groups, and the private sector. NICE leverages partnerships with these stakeholders to realize each goal.
STEM	Federal acronym for science, technology, engineering, and mathematics.

Appendix D. Acronyms

Acronym	Definition
CNCI	Comprehensive National Cybersecurity Initiative
DHS	Department of Homeland Security
DoC	Department of Commerce
DoD	Department of Defense
ED	Department of Education
IT	Information Technology
PreK-12	Pre-Kindergarten through 12th grade
NICE	National Initiative for Cybersecurity Education
NICS	National Institute for Cybersecurity Studies
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
ODNI	Office of the Director of National Intelligence
OPM	Office of Personnel Management
SLTT	State, Local, Tribal and Territorial governments
STEM	Science, Technology, Engineering, and Mathematics

Appendix E. Additional Resources

Topic	Web site
Comprehensive National Cybersecurity Initiative (CNCI)	http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure	http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
FISMA Implementation Project	http://csrc.nist.gov/groups/SMA/fisma/index.html
Cyber Tours	http://stopthinkconnect.org/cybertoursprogram/atlanta
National Centers of Academic Excellence	http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml
National Initiative for Cybersecurity Education (NICE)	http://csrc.nist.gov/nice/
National Cybersecurity Workforce Framework	http://csrc.nist.gov/nice/framework/
Scholarships For Service	http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5228 https://www.sfs.opm.gov/
Stop.Think.Connect.™ Campaign	http://www.dhs.gov/stopthinkconnect