National Initiative for Cybersecurity Education Strategic Plan

Building a Digital Nation

August 11, 2011

Table of Contents

Executive Summary

Our nation is at risk. The cybersecurity vulnerabilities in our government and critical infrastructure are a risk to national security, public safety, and economic prosperity. Now is the time to begin a coordinated national initiative focused on cybersecurity awareness, education, training, and professional development. The United States must encourage cybersecurity competence across the nation and build an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of threats.

This document represents the first strategic plan for the National Initiative for Cybersecurity Education (NICE) and will be updated in subsequent years as the initiative moves forward. This publication is intended to be read by a wide variety of Americans including everyday citizens whose daily lives interact with cyberspace, our students, our educators, chief information officers, chief human capital officers, our entrepreneurs, and those protecting online information, transactions, and processes.

The mission of NICE is to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace for all.

The vision of NICE is a secure digital nation capable of advancing America's economic prosperity and national security in the 21st century through innovative cybersecurity education, training, and awareness on a grand scale.

NICE will achieve this vision through the implementation of three goals:

1. Raise awareness among the American public about the risks of online activities.
2. Broaden the pool of skilled workers capable of supporting a cyber-secure nation.
3. Develop and maintain an unrivaled, globally competitive cybersecurity workforce.

This report describes NICE's strategic goals and their supporting objectives. These goals provide a framework for executing the initiative's mission and achieving its vision. The objectives provide high-level actions to be taken to achieve each of the goals. The outcomes for each objective allow NICE to measure progress in meeting its objectives. The strategies for each objective describe a way forward or mechanism to be used to meet each objective. This plan will provide a path to a more secure digital nation.

I. Introduction

Strategic Context

Our critical infrastructure – such as the electricity grid, financial sector, and transportation networks that sustain our way of life – has suffered repeated cyber intrusions, and cyber crime has increased dramatically over the last decade. The President has thus made cybersecurity an Administration priority. When the President released his Cyberspace Policy Review almost two years ago, he declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."

To protect and defend the nation's digital information and infrastructure, the United States must encourage cybersecurity competence across the nation and build an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of threats.

Purpose

The NICE Strategic Plan identifies goals and objectives that will contribute to the realization of a cyber-secure public and a globally competitive cybersecurity workforce.

NICE Mission

NICE will enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population.

NICE Vision

A secure digital nation capable of advancing America's economic prosperity and national security in the 21st century through innovative cybersecurity education, training, and awareness on a grand scale.

NICE Goals

1. Raise awareness among the American public about the risks of online activities.
2. Broaden the pool of skilled workers capable of supporting a cyber-secure nation.
3. Develop and maintain an unrivaled, globally competitive cybersecurity workforce.

NICE Stakeholders

NICE stakeholders span the breadth of American society from high-level government officials to individual American citizens. Every Internet user has a role to play in securing cyberspace and ensuring the safety of ourselves, our families, and our communities online, so individual American citizens are key stakeholders.

Key stakeholders exist within federal, state, local, tribal, and territorial governments and within the associations established to support the sharing of cybersecurity training, education, and awareness information.

Key stakeholders in the NICE initiative within the private sector include critical infrastructure owners/operators, large companies, small businesses, academic institutions, and other interested parties.

NICE Partnerships

Stakeholders have a special connection to NICE and are interested in how the initiative will impact them. Many NICE stakeholders are already actively involved in planning, administering, and deploying activities that support the goals of the initiative. These efforts, as well as many others, are critical to the effective implementation of NICE. It is critical, therefore, that partnerships with active stakeholders be promoted and that new partnerships be established to forge working relationships, leverage efforts across the nation, and maximize the impact of stakeholder activities. The partnerships contribute directly to the NICE goals and objectives through integrated educational, awareness, and workforce development activities.

Partnerships will be formed across stakeholder organizations, such as business, government, and academia, as shown in the following diagram. Together, the partners will build on their combined strengths and capabilities to produce greater and more sustainable impact and add value to what each can achieve alone. Cooperation among partners is voluntary, multidirectional, participative, trusted, sustainable, and supportive of the flow of information and ideas. Partnership engagement is vital to NICE planning, implementation, and evaluation to ensure that its activities are appropriate, effective, and sustainable.

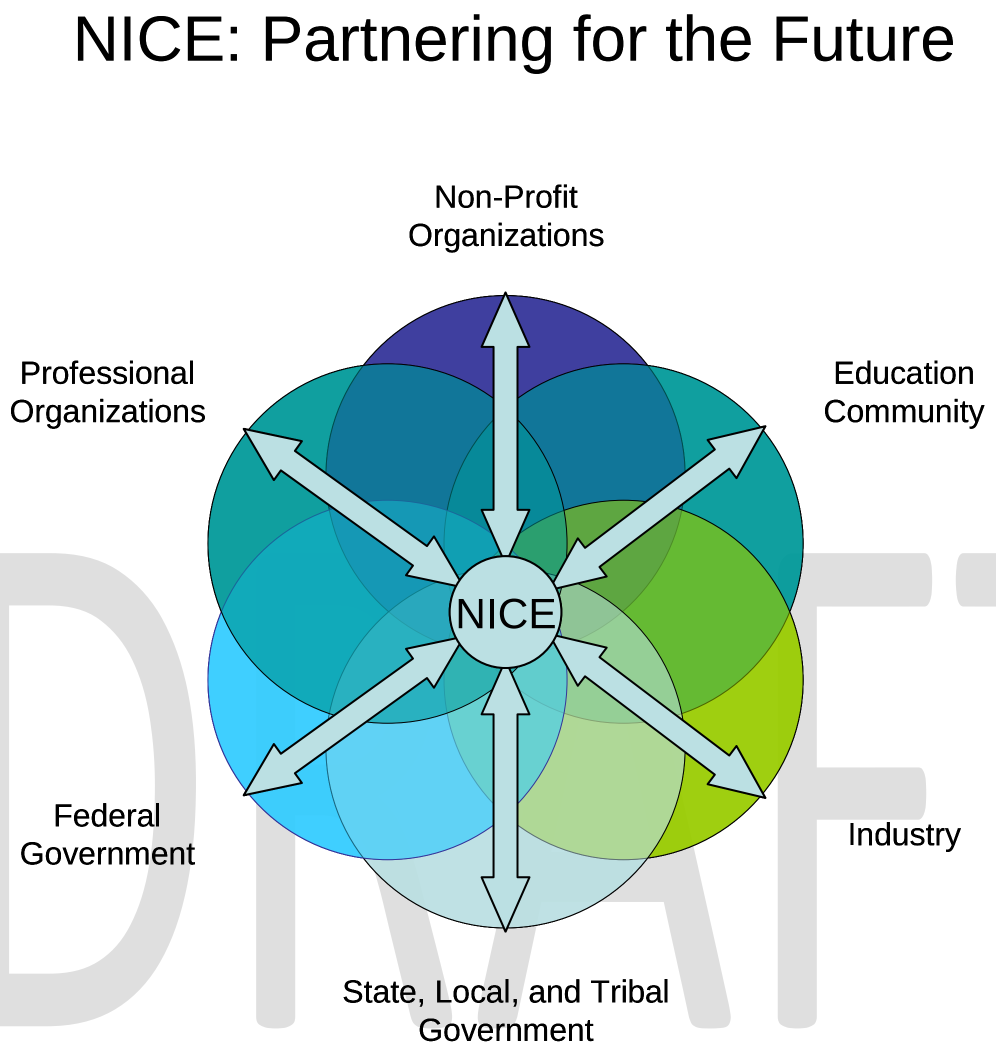
NICE: Partnering for the Future
Non-Profit Organizations
Professional Organizations
Education Community
NICE
Federal Government
Industry
State, Local, and Tribal Government

Figure 1: NICE Partnerships

Government Participants

As the designated lead for this initiative, the National Institute of Standards and Technology (NIST) will promote the coordination of existing and future activities in cybersecurity education, training, and awareness to enhance and multiply their effectiveness. It is envisioned that the Department of Homeland Security (DHS), the Department of Defense (DoD), the Department of Education (ED), NIST, and the National Science Foundation (NSF) will have major responsibilities for Goal 1; DHS, ED, NIST, NSF, and the National Security Agency (NSA) will have major responsibilities for Goal 2; and DHS, DoD, ED, NIST, NSA, NSF, and the Office of Personnel Management (OPM) will have major responsibilities for Goal 3.

II. NICE Strategic Overview

NICE is a multidimensional initiative whose aim is to institutionalize the nation's digital literacy and cybersecurity knowledge. This NICE strategic plan provides a spectrum of national cybersecurity knowledge spanning from informing the public to professional employment and development. The goals and objectives in the following sections focus on three overarching outcomes:

- Increase public awareness of cybersecurity risks, responsible use of the Internet, and cybersecurity as a career path;
- Develop the next generation of cybersecurity workers and encourage interest in science, technology, engineering, and mathematics (STEM) disciplines; and
- Raise the competency and capability of information security professionals and practitioners through education, training, employment, and certification.

Figure 2 illustrates how the elements of the spectrum link to NICE goals and overall strategic outcomes.

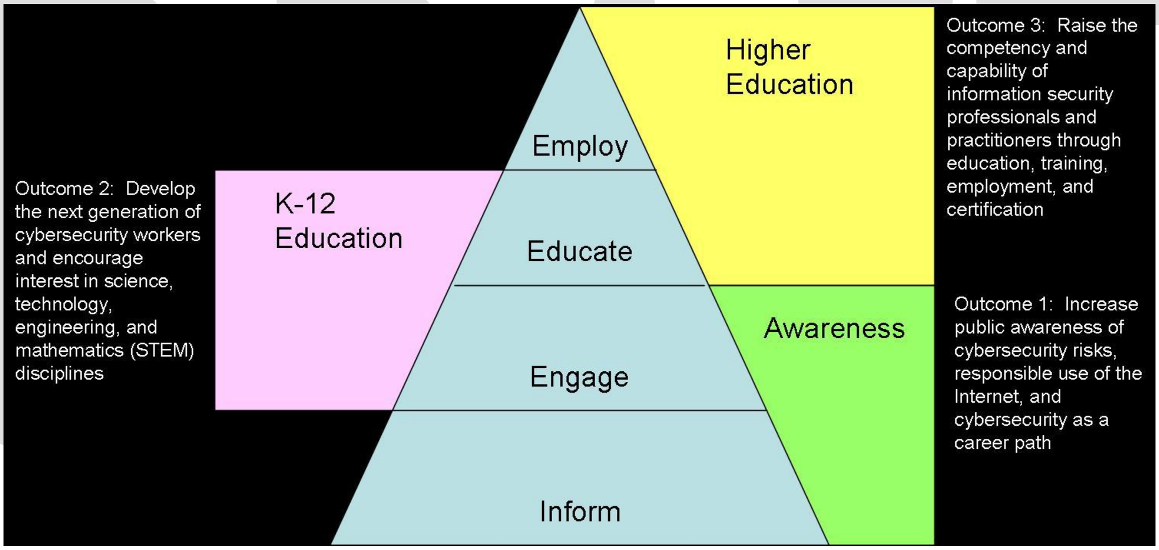
Outcome 2: Develop the next generation of cybersecurity workers and encourage interest in science, technology, engineering, and mathematics (STEM) disciplines
K-12 Education
Employ
Educate
Engage
Inform
Higher Education
Awareness
Outcome 3: Raise the competency and capability of information security professionals and practitioners through education, training, employment, and certification
Outcome 1: Increase public awareness of cybersecurity risks, responsible use of the Internet, and cybersecurity as a career path

Figure 2: Strategic Outcomes

The evolution to a national initiative drives the necessity to engage in a strategic planning process for NICE that leverages the activities of the NICE stakeholders, partners, and government. Stakeholders at the federal, state, local, tribal, and territorial levels, as well as academia and industry, have offered input to the planning process. This overall strategic plan is a dynamic document that will be updated in subsequent years to reflect new priorities, accomplishments, input, and information.

Table 1 introduces the NICE Strategic Goals and Objectives. Section III elaborates on each goal and objective.

Goal	Objective
1. Raise awareness about the risks of online activities.	1.1. Improve citizens' knowledge to allow them to make smart choices as they manage online risk.
	1.2. Improve knowledge of cybersecurity within organizations so that resources are well applied to meet the most obvious and serious threats.
	1.3. Enable access to cybersecurity resources.
2. Broaden the pool of skilled workers capable of supporting a cyber-secure nation.	2.1. Improve K-12 Science, Technology, Engineering, and Mathematics (STEM) education emphasizing the important role of mathematics and computational thinking.
	2.2. Increase the quantity and quality of academic computer science courses in high schools.
	2.3. Increase the quantity and quality of undergraduate and graduate cybersecurity curricula for students in computer science and, more broadly, IT and security-related degree programs.
	2.4. Incentivize, support, and recognize excellence in graduate-level cybersecurity research and development.
3. Develop and maintain an unrivaled, globally competitive cybersecurity workforce.	3.1. Develop a usable cybersecurity competency framework (Human Resources & Curriculum focus).
	3.2. Provide a framework for focusing cybersecurity training to meet evolving needs.
	3.3. Study the application of professionalization, certification, and licensing standards on cybersecurity career fields.

Table 1: NICE Strategic Goals and Objectives

For the remainder of this strategy, “cybersecurity workforce” is used to denote positions and people whose jobs are primarily focused on cybersecurity. For instance, while it will be beneficial for a nurse updating a patient’s electronic healthcare record to have cybersecurity training to perform his or her job and protect the patient’s privacy by following cybersecurity policies, the hospital where the nurse works will have employees or contractors whose primary job is planning, implementing, and maintaining the cybersecurity posture of the hospital’s systems. The nurse is part of our nation’s workforce that will benefit from Goal 1 awareness activity. The employees or contractors supporting the hospital’s cybersecurity are part of the “cybersecurity workforce.” Goal 3 is focused on the specialized skills of the “cybersecurity workforce.” Goal 2 aims at formal education that will prepare more people to enter into cybersecurity careers.

III. NICE Goals

This section describes the NICE strategic goals and supporting objectives in detail. These goals provide a framework for executing the NICE mission and achieving its vision. The objectives identified within each goal provide high-level actions that must be taken to achieve the NICE strategic goals. The strategies describe a way forward to meet each objective, while the outcomes allow NICE to measure progress in meeting its objectives.

Goal 1: Raise awareness about the risks of online activities.

The American public has grown increasingly dependent on online activities to manage all aspects of daily life and remains largely unaware of the risks threatening their privacy, safety, and financial security. Organizations, whose primary purpose is not focused on cybersecurity, are increasingly being drawn into conducting their business online without complete awareness of the risks of doing so. Online, as discussed here, indicates a state of connectivity most often with the Internet. This initiative needs to make more people aware that malicious actors exist and are ready to take advantage of people’s willingness to accept information from or provide personal information over the Internet. Included in this goal will be public messages that promote responsible use of the Internet and awareness of fraud, identity theft, cyber predators, and cyber ethics. Goal 1 aims to raise awareness about the risks of online activities at home, in the workplace, and in our communities.

Figure 3 displays the cybersecurity knowledge stages that NICE aims to achieve for individuals and organizations. Stage 1 – Awareness of the cybersecurity problem, everyone is at risk; Stage 2 – Understanding of the problem, technical and social aspects; Stage 3 – Recognizing personal responsibility, that everyone should and must do; Stage 4 – Acquiring protection tools and knowledge, accessing resources to gain ability to act; Stage 5 – Implement tools and techniques, putting into place the knowledge and tools acquired; and Stage 6 – Maintaining, continuous learning and responding to changing threats.

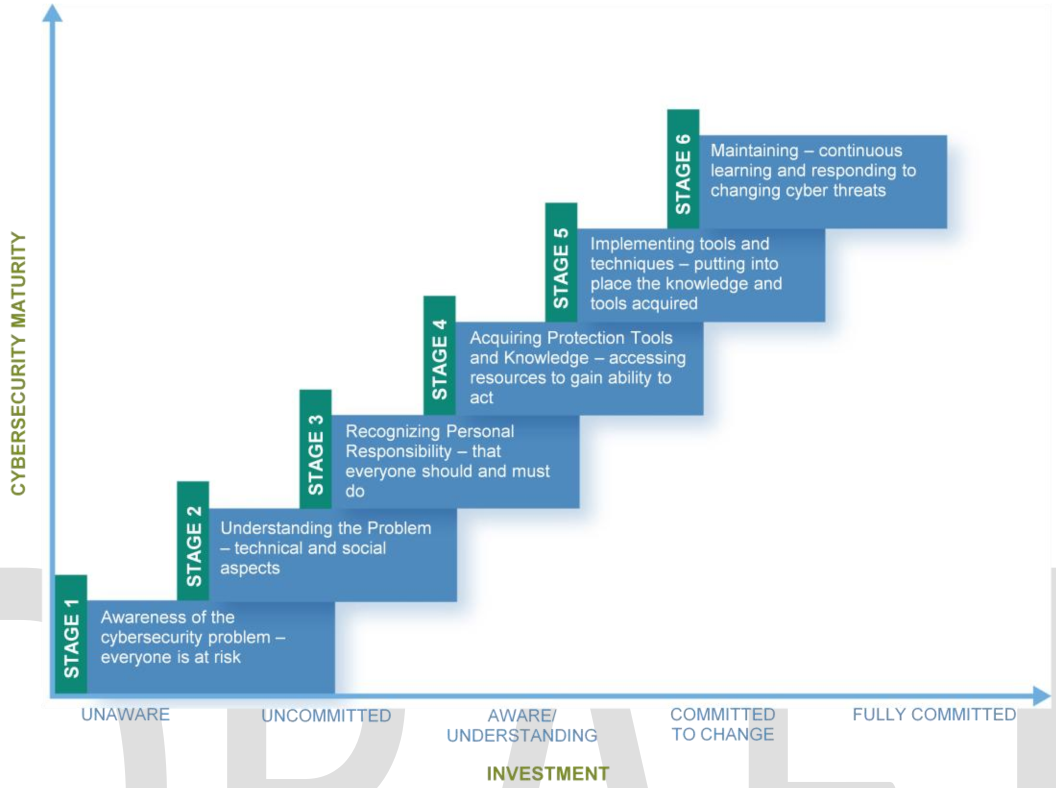
CYBERSECURITY MATURITY
STAGE 1
Awareness of the cybersecurity problem – everyone is at risk
STAGE 2
Understanding the Problem – technical and social aspects
STAGE 3
Recognizing Personal Responsibility – that everyone should and must do
STAGE 4
Acquiring Protection Tools and Knowledge – accessing resources to gain ability to act
STAGE 5
Implementing tools and techniques – putting into place the knowledge and tools acquired
STAGE 6
Maintaining – continuous learning and responding to changing cyber threats
UNAWARE
UNCOMMITTED
AWARE/ UNDERSTANDING
COMMITTED TO CHANGE
FULLY COMMITTED
INVESTMENT

Figure 3: Cybersecurity Knowledge

Goal 1 is supported by three objectives. Objective 1.1 is aimed at the American citizen, Objective 1.2 is aimed at the organizations where we work, and Objective 1.3 is aimed at enabling access to the resources needed by citizens and organizations.

Objective 1.1: Improve citizens' knowledge to allow them to make smart choices as they manage online risk.

The public is insufficiently aware of the risk of sharing information in cyberspace--which can affect personal and national security. Americans must be made more aware of the tools and practices that can help protect them from the negative consequences that cyber threats represent.

Cyberspace is defined as the interdependent network of information technology infrastructures, and 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. *Cyberspace Policy Review*

Figure 3 displays a multistage approach to reach the goal of increasing cybersecurity knowledge. NICE is focused on increasing the number of Americans in each of these stages and aims to promote awareness programs that support each stage.

Outcomes

Successful achievement of Objective 1.1 will result in the following outcomes:

- Citizens reduce fraud victimization resulting from online activity.

- Citizens consider the security privacy implications before sharing information online.
- Citizens increase implementation of tools that mitigate cyber threats.
- Citizens are increasingly aware of cybersecurity, with its precepts as prevalent as the awareness of the hazards of smoking, the wisdom of wearing seatbelts, and the physical benefits of good diet and exercise.

Strategies

- Awareness campaigns starting with STOP. THINK. CONNECT.[1]
- Develop standards and strategies for digital literacy training for the American population to ensure that the public can use the tools and techniques that reduce risk in the cyber environment.
- Deliver resources that enable educators to competently communicate cybersecurity awareness to students during all classroom interactions with cyberspace.
- Communicate the changing cyber threat landscape to citizens through a variety of outlets, including the awareness campaign, public service announcements, technical conferences, business roundtables, the Internet, and other media channels.

Objective 1.2: Improve knowledge of cybersecurity within organizations so that resources are well applied to meet the most obvious and serious threats.

Americans operate in a world where innovative cyber criminals invent new and sophisticated techniques that undermine the security of organizations. Because these threats change and evolve, it is imperative that these changes be tracked and that organizations be informed of current risks and mitigation techniques. Through education, training, and awareness campaigns, organizations should have the opportunity to learn about the many options for improving the cyber protection of intellectual property, customer data, services, and critical infrastructures as well as the development of improved cybersecurity tools and practices.

Figure 3 displays a multistage approach to reach the goal of increasing the cybersecurity knowledge maturity of the private sector. While not all private sector organizations may start in the same stage or possess the resources to allow them to reach Stages 4-6, Objective 1.2 aims to help all organizations improve their cybersecurity awareness. NICE aims to encourage private sector organizations to examine their cybersecurity risks so that they can make informed decisions about acquiring, implementing, and maintaining a cybersecurity posture to manage those risks.

Awareness resources aimed at organizations can also influence those organizations that build and sell technologies that connect to cyberspace. Objective 1.2 seeks to engage our nation’s innovators to consider cybersecurity at the earliest stages of design. Objective 1.2 includes in its aim to make today’s innovators aware of the tools and best practices available from today’s cybersecurity experts which could have an impact in making their products more competitive worldwide. Goal 2 described later in this document aims to encourage formal education to create more cybersecurity subject matter experts in the future.

Outcomes

Successful achievement of Objective 1.2 will result in the following outcomes for the private sector:

[1] www.dhs.gov/stopthinkconnect

- Increased awareness of the technical issues and threats leading to acquiring tools and training as necessary;
- Promotion of cybersecurity awareness to all employees;
- Protection of assets, functions, reputation, and operating capabilities;
- Promotion of privacy awareness to employees;
- Building of software and hardware having considered security implications;
- Increased quality of cybersecurity products and services available to the American public;
- Increased awareness of supply chain vulnerabilities; and
- Adoption of cybersecurity tools in support of product development.

Strategies

- Communicate the changing cyber threat landscape to private sector organizations through a variety of outlets, including the awareness campaign, public service announcements, technical conferences, business roundtables, the Internet, and other media channels.
- Communicate options for cyber protection, such as using security tools and training, educating the workforce, tracking demand, and promoting best practices and cybersecurity standards.
- Offer cybersecurity knowledge to small businesses and organizations.

Objective 1.3: Enable access to cybersecurity resources.

Americans lack authoritative, affordable, and readily accessible sources of information on which they can depend to help them distinguish cybersecurity hype from fact and good tools from bad ones. Government, academia, and industry need to work together to provide resources and tools that can help Americans stay safe online and strengthen our collective cybersecurity efforts.

Outcomes

Successful achievement of Objective 1.3 will result in the following outcomes:

- Increased availability of resources to obtain timely information and corroborate information; and
- Increased implementation of tools that mitigate cyber threats.

Strategies

- Partner with the private sector, academic institutions, and state/local/tribal/territorial governments to disseminate tools, training, and resources.
- Create, disseminate, and promote cybersecurity best practices and guidance in partnership with IT policy and directive organizations.

Goal 1 Supporting Activities and Products

- NICE Web site
- National Institute for Cybersecurity Studies (NICS) Portal
- Cyber Citizens Forums, Cyber Security Awareness Volunteer Education (C-SAVE) Project, and other volunteer programs
- National Cybersecurity Awareness Campaign: STOP. THINK. CONNECT[2]
- National Cybersecurity Awareness Challenge[3]

[2] http://www.stopthinkconnect.org/

[3] http://www.dhs.gov/files/cyber-awareness-campaign.shtm

Goal 2: Broaden the pool of skilled workers capable of supporting a cyber-secure nation.

The academic pipeline shown in Figure 4 describes transitions into the cybersecurity roles needed for Building Capacity for a Digital Nation called for in the President's Cyberspace Policy Review. Goal 2 aims squarely at formal education to increase the number of people with the cybersecurity skills necessary to meet the nation's cybersecurity needs.

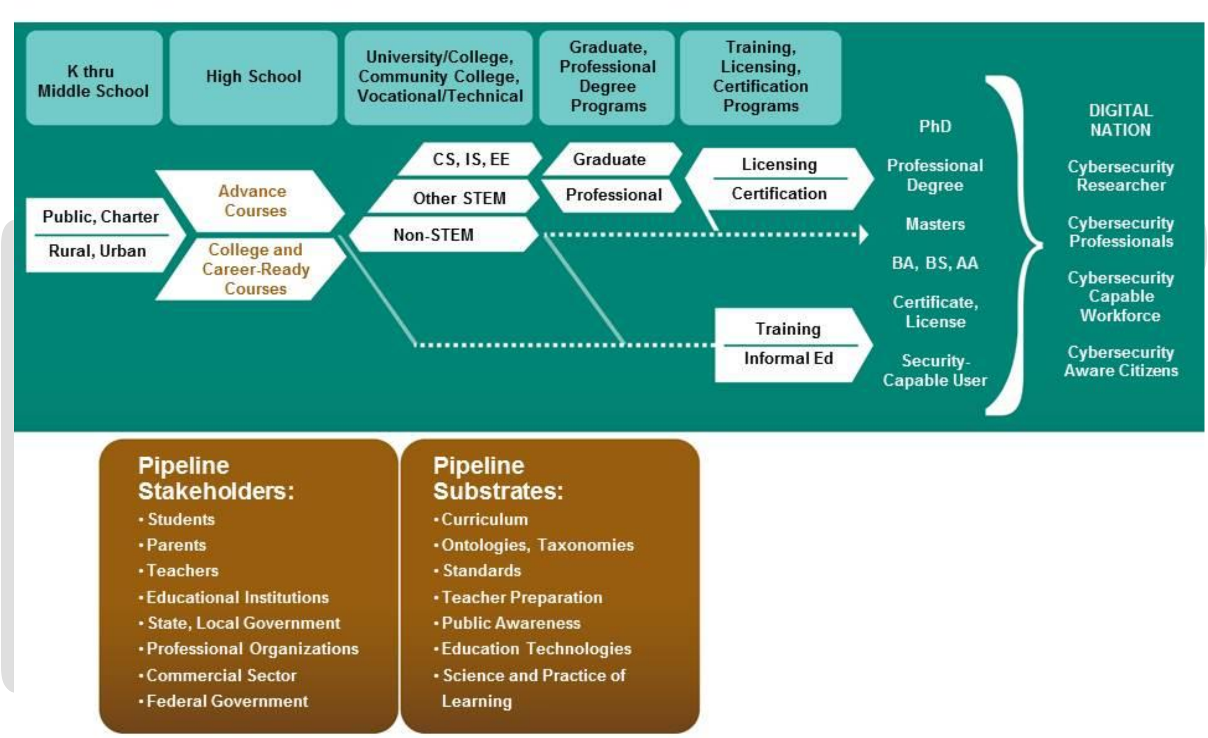

Figure 4: Cybersecurity Education and Training Pipeline

Our nation's education system can produce the next generation of cybersecurity experts by supporting a student's strong interest in mathematics beginning in elementary school and maintaining that interest through middle school. In high school, our nation's education system needs to create opportunities to explore computational thinking preparing more students who can take advantage of undergraduate and later graduate studies in cybersecurity. All this activity aims at leveraging work begun by the U.S. government working together with teachers, parents, students, and businesses to improve science, technology, engineering, and math (STEM) education to better prepare students to lead in the 21st century economy.

Objective 2.1: Improve K-12 STEM education emphasizing the important role of mathematics and computational thinking.

The academic pipeline begins with STEM, particularly mathematics education, in elementary and secondary school. Today, U.S. high school students are often well behind their international peers in

The effort to produce the next generation of cybersecurity professionals will need to build on a foundation of a strong STEM curriculum.

mathematics and science performance. Despite many national, state, and local efforts to improve STEM performance, much remains to be done.

Outcomes

Successful achievement of Objective 2.1 will result in the following outcomes:

- Within the next decade, U.S. students will move from the middle to the top of the pack in international assessments.
- An increased number of students will leave the 12th grade with the desire and capacity to pursue cybersecurity majors/careers.

Strategies

- Starting with FY13, align federal kindergarten through 12th grade (K-12) STEM education efforts to a coherent strategy.[4]
- Starting with FY13, align formal federal cybersecurity education budgets with the NICE strategic plan.
- Develop capacity to assist private entities who produce computer science and cybersecurity instructional materials, tools, and resources for K-12 STEM instruction with mechanisms for implementation at the state and district level.
- Assist corporations and foundations with (1) organizing around formal computer science education efforts at the state level, (2) educating their employees/partners about the needs for better education in general and computer science education in particular, and (3) becoming better at making evidence-based contributions to STEM education reform.
- Help the cybersecurity workforce to partner with local schools, thus providing content expertise to teachers and role models to students.

Objective 2.2: Increase the quantity and quality of academic computer science courses in high schools.

Most high schools do not offer rigorous academic computer science (CS) courses. Instead, high school computing courses are often focused on keyboarding and the use of standard office products. They train students to be users of technology, but not creators of technology, not adaptors of technology who can bend computation to their own ends. Few states have adopted K-12 computing education standards and few have a credentialing process for computer science teachers. In all but nine states, CS courses do not count toward mathematics or science graduation requirements. Worse, the trend is not positive. The Computer Science Teachers Association[5] reports that since 2005, schools are teaching 17 percent fewer introductory CS courses and 33 percent fewer Advanced Placement CS courses.[6]

As a result, most students arrive at college with little understanding of computer science, little understanding of the intellectually challenging problems computer science involves, and little understanding of the issues and potential careers in cybersecurity. Not surprisingly, few students choose to pursue information technology (IT) careers. Since 2000, the percentage of college freshman intending to major in computing has dropped by 70 percent;[7] this statistic is particularly true of women, minorities, and persons with disabilities. The National Science Foundation works to address this issue by

[4] This is being coordinated by the National Science and Technology Committee on STEM Education, chaired by The Office of Science and Technology Policy (OSTP) and NSF.

[5] csta.acm.org/

[6] Computer Science Teachers Association, National Secondary Computer Science Survey 2009

[7] Higher Education Research Institute, Freshman Survey 2009

supporting the College Board in development of a proposed new Advanced Placement (AP) course, called Computer Science Principles. This course will include an introduction to cybersecurity in the context of a more rigorous and engaging high school computer science curriculum.

Outcomes

Successful achievement of Objective 2.2 will result in the following outcomes:

- By 2018, 50 percent of high schools nationwide will offer rigorous academic computer science courses taught by well-prepared teachers.
- By 2018, there will be an increase in the number of students pursuing majors in computing at the postsecondary level.
- By 2018, 25 percent of the states will adopt national cybersecurity education standards for K-12.

Strategies

- Provide access to curriculum, materials, and assessments for high school computing courses that include cybersecurity, across a variety of "delivery trajectories" (e.g., 4th year mathematics courses, Career and Technical Education (CTE) course sequences, and the proposed new AP CS Principles course).
- Partner federal agencies with corporations and foundations to prepare and support high school computer science teachers, especially those teaching rigorous courses such as the proposed AP CS Principles course.

Objective 2.3: Increase the quantity and quality of undergraduate and graduate cybersecurity curricula for students in computer science and, more broadly, IT and cybersecurity-related degree programs.

Undergraduate cybersecurity curricula need to be developed that focus on coherent solutions comprising the effectiveness of integrated and coordinated security measures. To meet the cybersecurity needs of both public and private sectors, an undergraduate focus on cybersecurity needs to occur in an increasing percentage of the courses required for a bachelor or associate degree in computer science, computer engineering, software engineering, information systems, and information technology. Cybersecurity expertise cannot be developed in a single course on security, but rather needs to be a foundation of all coursework. Increasing the availability of graduate programs with a cybersecurity focus will provide opportunities to develop more expertise and will result in some students choosing to pursue doctorate degrees.

Outcomes

- An increased number of students receiving degrees that enable them to enter the cybersecurity field with the expertise needed by their employers.
- The National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) will review and update their standards and program criteria to meet evolving cybersecurity needs.
- By 2018, a 25 percent increase in the number of CAE-designated academic institutions focused on specific critical infrastructures, digital forensics, or other specializations.
- By 2018, a 20 percent increase in the number of accredited cybersecurity degree programs.
- By 2018, 20 percent of community colleges and technical schools will offer cybersecurity apprenticeships or certifications.

- By 2014, at least 150 undergraduate institutions will participate in the National Virtual Laboratory for Cybersecurity Education, National Institute for Cybersecurity Studies.

Strategies

- Provide postsecondary students with access to online cybersecurity courses/labs through access to the National Institute for Cybersecurity Studies (NICS) portal.
- Encourage public and private collaborations that create resource centers, such as the National Virtual Lab, providing infrastructure, content repositories, and faculty training.
- Increase the number of scholarships, fellowships, research experiences, and externships available to college and graduate students.
- Encourage the creation of accredited cybersecurity degree programs.
- Develop models for shared faculty, curricula, and virtual laboratories and make them easily accessible/publicly available.
- Fund capacity-building grant programs to institutions of higher education.
- Run competitions to create state-of-the-art distance learning/online course materials.

Objective 2.4: Incentivize, support, and recognize excellence in graduate-level cybersecurity research and development.

Research initiatives will drive the future development of cybersecurity solutions for the everyday computer user. Graduate-level cybersecurity research and development opportunities will draw students who are weighing their options about graduate programs to strongly consider cybersecurity for their academic career focus. Graduate-level cybersecurity research and development opportunities are a key part of developing the future academics capable of teaching future generations of cybersecurity students. Increasing the training and apprenticeship opportunities for graduate student cybersecurity researchers will support efforts to develop the game-changing technologies that can neutralize the attacks on the cyber systems of today and lay the foundation for a scientific approach that better prepares the field to meet the challenges of securing the cyber systems of tomorrow.

Outcomes

- Increase the availability of scholarships and fellowships.
- Increase access to dynamic learning environments such as virtualization and/or remote laboratories.
- Increase the number of universities designated as National Centers of Academic Excellence in Information Assurance Research (CAE-R).
- Increased opportunities to transition university research.

Strategies

- Identify and implement mechanisms that increase quantity and improve the quality of graduate research and development.
- Leverage Networking and Information Technology Research & Development (NITRD)[8] programs to create/support a government/academia/private industry forum that identifies problems for research.
- Align CAE-Rs with specific infrastructure sectors.

[8] http://www.nitrd.gov/

- Provide additional scholarships and fellowships for graduate students through collaborations with industry.
- Incentivize the external funding of student participation in professional conferences and exchanges.

Goal 2 Supporting Activities and Products

- The National Science Foundation's Computing Education for the 21st Century (CE21[9]) and 10,000 Computer Science teachers in 10,000 high schools (CS 10K[10]) programs, the Federal Cyber Service: Scholarship for Service (SFS[11]) programs, and the Advanced Technological Education (ATE[12]) programs
- The CAE/IAE program
- Competitions such as the National Collegiate Cyber Defense Competition[13] and National Science Bowl[14]

[9] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503582
[10] http://www.computingportal.org/cs10k
[11] https://www.sfs.opm.gov/
[12] www.nsf.gov/ate
[13] http://www.nationalccdc.org/
[14] http://www.scied.science.doe.gov/nsb/hs/students.htm

Goal 3: Develop and maintain an unrivaled, globally competitive cybersecurity workforce.

The exponential growth in the use of information technology represents both an asset and a vulnerability to the strength and prosperity of the nation that must be protected from attack and misuse. Technical solutions alone are not enough to ensure the safety and security of this essential infrastructure asset and the information that it contains. In addition to technology and infrastructure solutions, an agile, highly skilled professional cybersecurity workforce is required to secure, protect, and defend our nation’s information systems. Across America, private and public sector organizations have a pressing need for well-trained professionals to assess, design, develop, and implement cybersecurity solutions and strategies. The expanding need, however, is not met with a comparably expanding professional cybersecurity workforce.

Efforts to build our nation’s cybersecurity workforce incorporate three complementary components: workforce planning, professional development, and the identification of core professional competencies. **Workforce planning** analyzes the functional capabilities needed to achieve the current mission, forecast future capabilities, and identify specific knowledge, skills, and abilities for cybersecurity professionals. **Professional development** incorporates formal training and education to maintain the technical health of the cybersecurity workforce. Professionalization of cybersecurity **identifies core occupational competencies**, sets objective standards for skills development, accreditation, and job performance of cybersecurity practitioners, and develops career ladders within the various cybersecurity disciplines.

Leadership awareness of the critical and unique nature of cybersecurity work is needed to ensure that time and attention for workforce planning and professional development are initiated and sustained. A communication strategy and inclusion of cybersecurity challenges and responses will need to be part of leadership development programs. Managing a cybersecurity workforce will be part of organizational leadership at all levels.

Objective 3.1: Develop a usable cybersecurity competency framework.

Effective human capital planning enables our nation to have the right people, with the right skills, at the right time and place. The talent of the cybersecurity workforce is of significant concern across all business areas of the national landscape. The protection of the information infrastructure and the privacy of American citizens depend on the knowledge and abilities of this specialized workforce. As an emerging field, cybersecurity lacks a common terminology for career paths, position descriptions, and qualifications. A national cybersecurity competency framework is a prerequisite to effective human capital planning. Establishing such workforce definitions and standards would not only provide clarity for cybersecurity professionals but would also unify recruitment, placement, and performance assessment of these professionals. These definitions and standards, initially developed for use within the federal government and vetted by cyber and human capital subject matter experts, will be made available publicly, to public and private sector organizations, including state, local, tribal, and territorial governments, to apply as appropriate. Establishing definitions will be critical in order to measure and assess the cybersecurity workforce with any consistency.

Figure 5 represents a phased approach for building and implementing an organizational cybersecurity workforce capability and development model based on a national core competency framework.

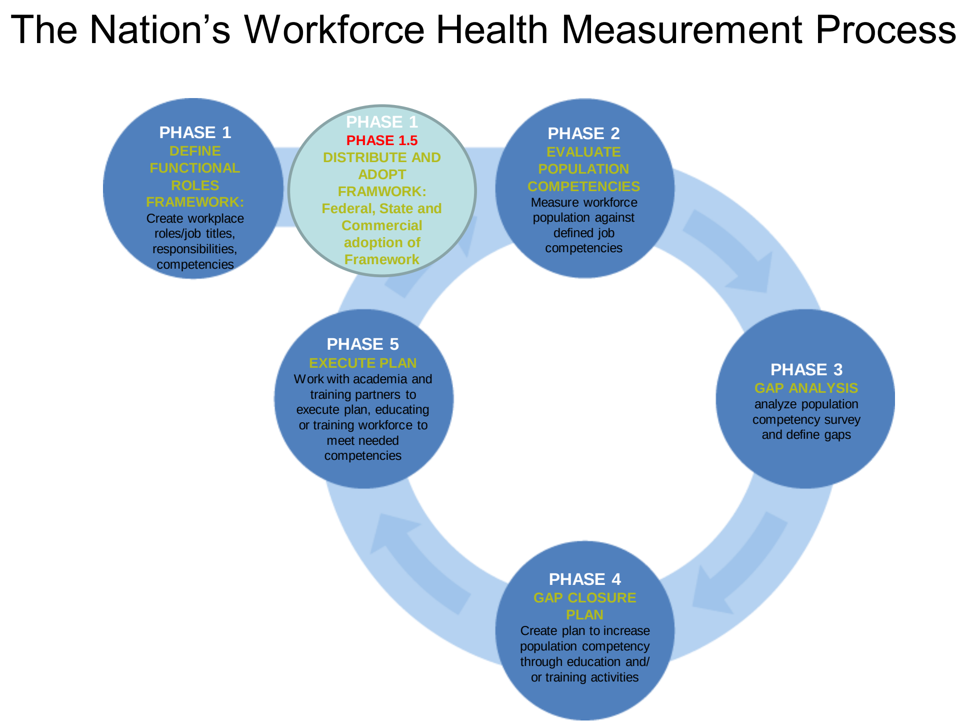
The Nation’s Workforce Health Measurement Process
PHASE 1
DEFINE FUNCTIONAL ROLES FRAMEWORK:
Create workplace roles/job titles, responsibilities, competencies
PHASE 1
PHASE 1.5
DISTRIBUTE AND ADOPT FRAMWORK:
Federal, State and Commercial adoption of Framework
PHASE 2
EVALUATE POPULATION COMPETENCIES
Measure workforce population against defined job competencies
PHASE 3
GAP ANALYSIS
analyze population competency survey and define gaps
PHASE 4
GAP CLOSURE PLAN
Create plan to increase population competency through education and/ or training activities
PHASE 5
EXECUTE PLAN
Work with academia and training partners to execute plan, educating or training workforce to meet needed competencies

Figure 5. Cybersecurity Workforce Capability and Development Model

A commonly accepted cybersecurity professional competency framework provides a baseline of knowledge, skills, and behaviors for professionals across the diverse array of cybersecurity disciplines and a foundation for the education and training necessary to excel in these careers. A competency framework also facilitates the identification of training needs and guides the design of a professional development program. Furthermore, a common framework can assist organizations in specifying knowledge, skill, and performance expectations; determining whether current and potential employees meet job-skill requirements without additional and/or recurring development activities; and by providing a model for assessing knowledge and skills, creating employee professional development plans.

Outcomes

- Standardized functional roles and competencies are publicly available.
- By 2012, federal agencies adopt cybersecurity competency models.
- Shortages and skill gaps for cybersecurity professionals are identified.
- By 2013, federal agencies address cybersecurity work in human resources guidance.
- By 2015, state, local, tribal, and territorial governments adopt common workforce descriptions.
- By 2015, an estimate of the health of the national cybersecurity workforce is produced.
- By 2015, industries seeking federal contracts adopt workforce descriptions.
- By 2015, industries map their cybersecurity workforce descriptions for available positions.
- By 2015, the workplace will see a 20 percent increase in qualified cybersecurity professionals.

Strategies

- By 2013, assess the strength of the federal, state, and local cybersecurity workforce against defined cybersecurity competencies.
- Develop a baseline of the skills necessary for the cybersecurity professional.
- By 2015, assess the capabilities of the private sector cybersecurity workforce against the projected market requirements.
- Encourage public and private collaborations to utilize cybersecurity competency frameworks.
- Work with academia and industry to determine new workforce requirements emerging from changing technology and threats.
- Encourage the improvement and advancement of cybersecurity occupational certification programs.
- Establish a baseline for cybersecurity professionals across multiple industry sectors.

Objective 3.2: Provide a framework for focusing cybersecurity training to meet evolving needs.

Training is a journey, not a destination, and continued professional development demands continued training; however, training programs for the professional cybersecurity workforce are inconsistent and may not fulfill the unique needs of this particular workforce segment. Specialized cybersecurity training must ensure that the cybersecurity workforce have the practical skills, resources, and credibility to fulfill their roles. A commonly accepted core training framework plays a vital role in ensuring workforce competency standards throughout the nation and providing consistency in training curriculum for new and established cybersecurity practitioners. The use of a standardized training framework will help to ensure that training is widely accessible and conducted in a consistent manner. In addition, as requirements on the cybersecurity workforce evolve, a standardized framework will help to ensure that training efforts are targeted to meet changing needs.

Outcomes

- A comprehensive world-class training program designed to meet the functional requirements of government and private sector organizations;
- Standardized training tools, tradecraft, and methodologies;
- A mechanism that enables government, academia, and industry to share cybersecurity experiences to improve and refresh training programs; and
- Aligned and integrated cybersecurity training programs at all levels.

Strategies

- Promote a comprehensive world-class training regime program designed to meet the functional requirements of the government and private sector organizations.
- Compile a comprehensive cybersecurity training catalog, and foster the development of new courses to fill identified gaps.
- Measure training against common standards, learning objectives, and level of difficulty.

Objective 3.3: Study the application of professionalization, certification, and licensing standards on cybersecurity career fields.

To protect our personal, public, and private sector information, information systems, and networks, our nation must develop a workforce with a common understanding of the concepts, principles, and applications of cybersecurity for each cyber career category, specialty, level, and function. The practices of cybersecurity are professional disciplines; to acknowledge the professional stature and accomplishments of persons in these disciplines and to improve the quality of practice, it is worthy to look towards defining the expected level of preparation, proficiency, and competence in a consistent and widely recognizable manner, such as professionalization, certification, or licensing. By setting objective standards for skill development, accreditation, and job performances, professionalization will provide a common understanding of the activities and capabilities of cybersecurity practitioners, as it has in other disciplines.

Outcomes

- Develop a well-documented and widely accepted career progression, complete with flexible, challenging, and rewarding career paths and tracks.
- Sustain cybersecurity professional status.

Strategies

- Study and examine the impact of professionalization on other career fields.

Goal 3 Supporting Activities and Products

- Federal Information Systems Security Educators' Association (FISSEA)[15]
- Virtual Training Environment (VTE)[16]
- Industry Associations
- Certification Consortiums
- Cooperative cybersecurity research and education organizations
- Leadership development programs that include management of the cybersecurity workforce as an organizational imperative

[15] http://csrc.nist.gov/organizations/fissea/home/index.shtml
[16] https://www.vte.cert.org/vteWeb/

IV. Communication and Outreach

NICE will undertake four communication and outreach activities to enable the effective implementation of the “Goals and Objectives” identified in the first three sections of this document. Activities will leverage all forms of media.

The four activities support NICE’s ability to utilize and establish public and private collaborations; participate in national cybersecurity education, training, and awareness engagement events; evolve cybersecurity education, disseminate training and awareness best practices, and formally encourage creativity and innovation; and provide coordination among stakeholder agencies.

Public-private sector partnerships

NICE will leverage existing public-private sector relationships which enable collaboration and information sharing between federal departments and agencies, state, local, tribal, and territorial governments, and the private sector in order to promote the importance of NICE and to provide opportunities for participation. NICE will identify gaps not covered in current partnerships and work within federal guidelines to create new public-private sector partnerships necessary to meet its goals and objectives.

Conferences, workshops, symposia, and cyber competitions

Federal departments and agencies, state, local, tribal and territorial governments, private sector partners, and academia use conferences, workshops, symposia, town hall meetings, and cyber competitions to meet their objectives. NICE envisions leveraging those activities to create awareness about the goals and objectives of NICE and opportunities within such activities for stakeholders to participate in meeting NICE goals and objectives.

Open Government

In the Memorandum on Transparency and Open Government,[17] issued on January 21, 2009, the President directed the Office of Management and Budget to issue an Open Government Directive, emphasizing the importance of disclosing information that “the public can readily find and use.” NICE will establish and maintain a Web site that will allow the public to readily find and use information about cybersecurity awareness and education.

Government repository

In addition to a public Web site, NICE will establish a mechanism within the government for coordination, communication, and the development of all government activities enabling NICE. This internal Web-based mechanism will house information that supports the ability of NICE to develop a shared message, to store reference materials, and to host databases needed to track NICE interactions.

[17] http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/

Appendix A: Policy References

The following policies form the basis for NICE:

- National Cybersecurity Education Initiative "Building Capacity for a Digital Nation" Recommendation for the Information and Communications Infrastructure - Interagency Policy Committee, March 2010

- Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) Summary of Conclusions, March 23, 2010

Federal departments and agencies collaborate on NICE under their own standing authorities.

Appendix B: The National Initiative for Cybersecurity Education (NICE) Leadership Plan

The National Initiative for Cybersecurity Education (NICE) Leadership Plan

26 OCTOBER 2010

Purpose: The document defines leadership responsibilities for the National Institute of Standards and Technology in its role as lead agency for the National Initiative for Cybersecurity Education (NICE).

NICE will enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace for all.

Background: NIST was designated as the lead for NICE in a March 2010 recommendation of the Information and Communications Infrastructure – Interagency Policy Committee (ICI-IPC). This recommendation was based on Chapter 2 of the May 2009 Cyberspace Policy Review titled “Building Capacity for a Digital Nation” and is responsive to President Obama’s declaration that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.”[18]

Leadership Role: As the designated lead, NIST will promote the coordination of existing and future activities in cybersecurity education, training, and awareness to enhance and multiply their effectiveness.

Leadership Responsibilities:

- **Managing a coherent program.** Program management for NICE is intended to increase the overall effectiveness of cybersecurity education, training, and awareness by leveraging strengths, eliminating duplication, and identifying and addressing gaps. In addition, program management provides a mechanism for coordination, communication, assessment, and the development of a shared vision.
    - ○ NIST will support the efforts of track leads and track members in their NICE activities, including facilitating meeting logistics, aiding in developing reports and other documents, and supporting the effective use of Web-based resources.
    - ○ NIST will facilitate the identification of conflicts, gaps, and points of mutual support and leverage; communicate findings from the evaluation; and encourage innovative approaches to address issues.

[18] http://www.whitehouse.gov/administration/eop/nsc/cybersecurity

  - NIST will develop and coordinate a comprehensive communications plan to ensure consistency and accuracy of the message(s) that NICE provides in all activities.
  - NIST will coordinate efforts to identify cyber risks and determine where effective cybersecurity education, training, and awareness will have the most impact.
  - NIST will coordinate the development, reporting, and tracking of measurements and metrics assessing effectiveness of cybersecurity education, training, and awareness.
  - NIST will coordinate the development of a strategic plan to guide future NICE activities among stakeholders and partners.
- **Championing the Initiative.** Move the emphasis on cybersecurity past solely technical solutions and approach it as commensurate with public safety or health. Expand the understanding of the importance of cybersecurity as a personal, national, and economic issue.
  - NICE leadership will coordinate and champion a national campaign on cybersecurity training, education, and awareness.
  - NIST will leverage its long-standing relationships with industry, academia, and the national and international standards development communities to ensure that the message of cybersecurity education, training, and awareness is promoted.
  - NICE leadership will work to complement related national initiatives and programs such as Science, Technology, Engineering, and Mathematics (STEM) education, Scholarships for Service (SFS), and the National Centers of Academic Excellence in IA Education (CAE/IAE) and CAE-Research (CAE-R) programs.
- **Providing Cybersecurity Resources.** Provide a forum for cybersecurity education, training, and awareness materials and tools.
  - NICE leadership will assist in the transfer of research and development (R&D) results and information across a range of cybersecurity education and training programs.
  - NIST, in concert with NICE leadership, will develop and promote guidelines for achieving and maintaining good cybersecurity.
  - NIST will deploy a portal as a tool for community engagement as a mechanism for transparent open communications and community input, including best practices.
- **Developing a Compelling Business Case.** Develop cybersecurity education, training, and awareness business cases that promote U.S. competitiveness in the global marketplace, by strengthening and safeguarding the nation's cybersecurity infrastructure; keep America competitive with cutting-edge science and technology and an unrivaled cybersecurity information base; and ensure sustainable economic opportunities.

- NIST will lead efforts to develop persuasive business cases that promote U.S. cybersecurity innovation and industrial competitiveness.

Leadership Structure:

NIST is establishing the following leadership structure for the NICE effort:

The NICE NIST Internal Management Council (NNIMC) consists of three senior members of NIST's Information Technology Laboratory (ITL): the Division Chief of ITL's Computer Security Division, the NIST/ITL Chief Cybersecurity Advisor, and the Group Manager for Security Management & Assurance. This team shall be responsible for the overall strategic plan and coordination and communication with senior Administration officials.

The NICE NIST Leadership Team (NNLT) consists of the NICE Program Manager, the NICE Communications Coordinator, and the NICE liaisons. This team shall implement the strategic plans, execute program management, conduct community engagements, evaluate measurements against metrics, develop and promote guidelines, and maintain the Web portal. They shall coordinate development of business cases and long-term sustainability efforts.

In addition, NIST will leverage its internal administrative resources as needed. These include the Public and Business Affairs Office, Conference Program Office, Congressional and Legislative Affairs Office, and the International and Academic Affairs Office.

Appendix C: Acronyms

Acronym	Definition
AP	Advanced Placement
ATE	Federal Cyber Service Advanced Technological Education program
CAE/IAE	National Centers of Academic Excellence in Information Assurance Education
CAE-R	CAE-Research
CE21	National Science Foundation’s Computing Education for the 21st Century
CS	Computer Science
CS 10K	National Science Foundation’s 10,000 Computer Science teachers in 10,000 high schools
C-SAVE	Cyber Security Awareness Volunteer Education Project
CTE	Career and Technical Education
DHS	Department of Homeland Security
DoD	Department of Defense
ED	Department of Education
FISSEA	Federal Information System Security Educators’ Association
ICI-IPC	Communications Infrastructure – Interagency Policy Committee
IT	Information Technology
ITL	NIST Information Technology Laboratory
K-12	Kindergarten through 12th grade
NICE	National Initiative for Cybersecurity Education
NICS	National Institute for Cybersecurity Studies
NIST	National Institute of Standards and Technology

NNIMC	NICE NIST Internal Management Council
NNLT	NICE NIST Leadership Team
NSA	National Security Agency
NSF	National Science Foundation
OPM	Office of Personnel Management
OSTP	Office of Science and Technology Policy
SFS	Federal Cyber Service Scholarship for Service
STEM	Science, Technology, Engineering, and Mathematics
VTE	Virtual Training Environment