



Securing America's digital infrastructure through education |

Bill Newhouse



On May 29, 2009, in the East Room of the White House, President Barack Obama announced that his administration will pursue a new comprehensive approach to securing America's digital infrastructure. During the speech on "Securing our nation's cyber infrastructure," [1] he noted the following:

... we will begin a national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms, and to build a digital workforce for the 21st century. And that's why we're making a new commitment to education in math and science, and historic investments in science and research and development. Because it's not enough for our children and students to master today's technologies—social networking and emailing and texting and blogging—we need them to pioneer the technologies that will allow us to work effectively through these new media and allow us to prosper in the future.

“Building capacity for a digital nation,” part II of the president’s cyberspace policy review [2], included recommendations around the idea that the general public needs to be well informed to use technology safely, that the US needs a technologically advanced workforce to remain competitive in the twenty-first century economy, and that math and science must be a priority in schools. The review suggested that the US 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. To help achieve these goals, the review stated that the nation should:

- ▶ Promote cybersecurity risk awareness for all citizens;
- ▶ Build an education system that will enhance understanding of cybersecurity and allow the US to retain and expand upon its scientific, engineering, and market leadership in information technology;
- ▶ Expand and train the workforce to protect the nation’s competitive advantage; and
- ▶ Help organizations and individuals make smart choices as they manage risk.

In response to the president’s cyberspace policy review, the National Security Staff (NSS)’s Cybersecurity Directorate and the Office of the Director of National Intelligence (ODNI)’s Joint Interagency Cyber Task Force formed an interagency working group to expand the Comprehensive National Cybersecurity Initiative (CNCI)’s initiative #8—Expand Cyber Education—to encompass a national, rather than federal, focus. The goal of the working group was to formulate a recommendation for the Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) on a way forward for a national program to improve cybersecurity awareness, education, workforce structure, and training.

The working group consisted of representatives from the NSS Cybersecurity Directorate staff; ODNI; the Departments of Commerce, Defense (DoD), Education, Homeland Security (DHS), Justice (DoJ), Labor (DoL), State, and Treasury; NSA; the Office of Personnel Management (OPM); the Office of Management and Budget; and the Office of Science and Technology Policy. The group worked for several months to finalize a recommendation to the ICI-IPC

on the governance model for a national cybersecurity education program. The recommendation resulted in the March 2010 creation of an interagency structure and governance model for the National Cybersecurity Education Initiative, renaming it the National Initiative for Cybersecurity Education (NICE) [3].

National Initiative for Cybersecurity Education (NICE)

With NICE, the federal government aims to enhance the overall cybersecurity posture of the US by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population. This will enable a safer cyberspace for all. The initiative has established three underlying goals:

- ▶ Raise national awareness about risks in cyberspace,
- ▶ Broaden the pool of individuals prepared to enter the cybersecurity workforce, and
- ▶ Cultivate a globally competitive cybersecurity workforce.

The recommendation identified the National Institute of Standards and Technology (NIST) as the overall lead with four components (shown in figure 1).

Interagency structure

NICE will be represented by the following four components.

1. National cybersecurity awareness campaign.

The goal of this component, led by DHS, is to improve the cybersecurity behavior of the American public. DHS is doing this by delivering a national public awareness campaign—Stop.Think.Connect. [4]—aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. A core strategy of the campaign is a National Cyber Awareness Coalition [5], which comprises federal agency partners as well as state and local governments. The Coalition offers a mechanism for message and materials dissemination. Making effective use of the communications channels and outreach capabilities of the Coalition members is key to extending

the campaign's reach. Projects within this component include:

- » Planning and executing Cyber Tours [6] nationwide to directly engage communities in promoting awareness and initiating a dialogue about the dangers individuals face online;
- » Launching and expanding the National Network, a spin-off of the National Cyber Awareness Coalition, which will mirror the Coalition but be open for membership from any national nonprofit organization;
- » Improving the Stop.Think.Connect. resources, such as the Toolkit [7];
- » Finding new outreach opportunities and mechanisms to spread the campaign's message; and
- » Increasing coordination of the campaign and National Cyber Security Awareness Month (NCSAM), including incorporating Stop.Think.Connect. language in the state proclamations and conducting a Cyber Tour during NCSAM.

2. Formal cybersecurity education. The goal of this component, led by the Education Department and National Science Foundation (NSF), is to broaden the pool of skilled workers for a cyber-secure nation. It is responsible for supporting formal education to increase both the number of people with cybersecurity knowledge, skills, and abilities and the quality of the cybersecurity capabilities held by those people. Projects within this component include:

- » Making the connection between cybersecurity and science, technology, engineering, and mathematics (STEM);

- » Disseminating common evidence standards in pre-K–12 education;
- » Promoting the growth of effective cybersecurity competitions in high schools and higher education;
- » Facilitating the development of curricular recommendations in high schools and higher education; and
- » Coordinating a learning network of virtual national cybersecurity laboratories.

3. Cybersecurity workforce structure. The goal of this component, led by DHS and supported by OPM, is to define cybersecurity jobs, attraction, recruitment, retention, and career path strategies. This component contains the following sub-component areas: the federal workforce (led by OPM), the government (nonfederal) workforce (led by DHS), and the private sector workforce (led by the Small Business Administration, DoL, and NIST).

This component focuses on talent management of cybersecurity professionals. It aims to evaluate the professionalization of the workforce, recommend best practices for forecasting future cybersecurity needs, and define national strategies for recruitment and retention. Projects within this component include:

- » **Professionalization**—establishing a methodology for identifying cybersecurity areas to be professionalized [8] and providing a central national resource for cybersecurity professionalization.
- » **Workforce planning**—delivering a methodology for accurately forecasting cybersecurity workforces across government, industry, and academia.



- » **Recruitment and retention**—providing, disseminating, and maintaining a strategy and set of materials for recruiting and retaining cybersecurity professionals at the national level.

4. Cybersecurity workforce training and development. The goal of this component, led by DHS, DoD, and ODNI, is to develop and maintain an unrivaled cybersecurity workforce. It contains the following functional areas: general IT use (led by DHS and the Department of the Navy); information technology infrastructure, operations, maintenance, and information assurance (led by DoD and DHS); domestic enforcement and counterintelligence (led by the Defense Cyber Crime Center, the Office of the National Counterintelligence Executive, DoJ, and the US Secret Service); and specialized cybersecurity operations (led by NSA).

This component is responsible for defining the cybersecurity workforce and identifying the training and professional development required for the nation's cybersecurity workforce. Projects within this component include:

- » **National Cybersecurity Workforce Framework [9]**—providing a common language to define cybersecurity work. The Framework defines specialty areas; knowledge, skills, and abilities (KSAs); and competencies.
- » **Training catalog/National Institute for Cybersecurity Studies portal**—serving as a national online resource for information about cybersecurity awareness, education, careers, and professional development. It provides an online web resource that has a robust and representative collection of training opportunities mapped to the National Cybersecurity Workforce Framework.
- » **Workforce inventory**—collecting data to baseline and identify the current state of the IT workforce and assess current cybersecurity capabilities.
- » **Training gap analysis**—ensuring that available training is appropriate in terms of quality, need, and content.

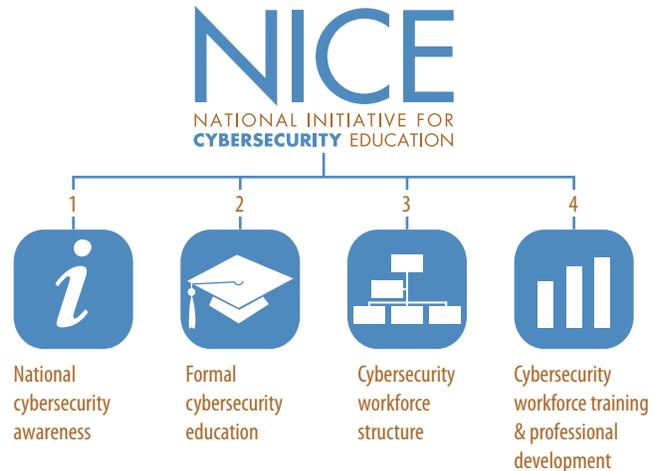


FIGURE 1. The National Initiative for Cybersecurity Education (NICE) is broken into four components aimed at enhancing the overall cybersecurity posture of the US.

- » **Professional development road maps**—developing resources which depict career progression from entry to expert within each specialty area.

Relationship to the cybersecurity R&D science of security thrust

In December 2011, the White House released “Trustworthy cyberspace: Strategic plan for the federal cybersecurity research and development program” [10] that included a thrust on developing scientific foundations. This thrust challenges the research and development (R&D) community to organize the knowledge in the field of cybersecurity and to investigate universal concepts that are predictive and transcend specific systems, attacks, and defenses resulting in a cohesive understanding of underlying principles of cybersecurity. This thrust will enable investigations that affect large-scale systems and will promote the development of hypotheses subject to experimental validation; it will also support high-risk explorations needed to establish a scientific basis and to form public-private partnerships of government agencies, universities, and industry.

NICE seeks to organize the knowledge in the field of cybersecurity education by supporting the development of cybersecurity awareness and educational content appropriate for different audiences and students.

NICE also seeks to identify and develop consensus on universal concepts that support increased cybersecurity awareness, expand cybersecurity education, and nurture a cybersecurity workforce that is prepared to support our nation's future.

NICE will continue to form public-private partnerships to achieve its goals. Leadership from the private and academic sectors is critical to the success of the NICE strategy to help organize disparate areas of knowledge. The R&D strategy noted that developing a strong, rigorous scientific foundation to cybersecurity helps the field by providing structure and organization to a broad-based body of knowledge in the form of testable models and predictions. This is true for NICE as well, but rather than testable models and predictions, NICE needs to develop common core state standards [11] for cybersecurity that will enable cybersecurity to be incorporated into K–12 education. The formation of cybersecurity education and awareness into a common core standard like the one already designed for mathematics [12] will help define what students should understand and be able to demonstrate in their study of cybersecurity.

Increased exposure to cybersecurity concepts, including computational thinking [13] in K–12 education, and an overall STEM emphasis in K–12 education will produce more students with the skills necessary to perform cybersecurity R&D as they matriculate through universities, academies, colleges, and institutes of technology. NICE believes that the innovative skills gained while performing R&D in an academic environment will translate into more people capable of performing and leading cybersecurity R&D activities within both the federal government and the nation's high-tech industries. NICE also recognizes the need to keep up with the innovations developed by the R&D community as the initiative continues its pursuit of its strategic goals.

The science of cybersecurity workforce

The National Cybersecurity Workforce Framework provides a common set of definitions for the cybersecurity workforce. The Framework brings consistency to how cybersecurity work is defined and described. It provides a common language to discuss and understand the work requirements of cybersecurity professionals, empowering our nation's agencies and industries to:

- ▶ Baseline capabilities,
- ▶ Identify skill gaps,
- ▶ Develop cybersecurity talent in the workforce, and
- ▶ Prepare the pipeline of future talent.

The Framework organizes the cybersecurity workforce into seven broad categories, then into thirty-one specialty areas. These specialty areas are further broken down into work roles and then KSAs. Some organizations may mix roles or specialty areas; this is a major strength for the Framework in that it can be customized to fit the needs of an organization and still maintain its integrity. The Framework was developed in collaboration with subject matter experts from government, nonprofits, academia, and the private sector.

The Framework concept began before the establishment of NICE and grew out of the recognition that the cybersecurity workforce (federal and private industry) could not be measured and that the roles needed to support our nation's cybersecurity were undefined. To combat this challenge, the federal Chief Information Officers (CIO) Council [14] began a Cybersecurity Workforce Development Matrix effort in 2008, when the organization was tasked to provide a standard framework to understand the cybersecurity roles within the federal government. In 2008, the CIO Council's Information Technology Workforce Committee (ITWC) conducted an environmental scan and produced a research report that referenced where other information technology professional development efforts were also underway, including the "Essential Body of Knowledge (EBK) report" and "The Committee of National Security Systems (CNSS) standards." Specific roles were identified as needed by agencies to conduct cybersecurity work.

In November 2011, thirteen roles were identified and four cybersecurity development matrices were published by the federal CIO Council along with the "Cybersecurity workforce development matrix resource guide" [15] to instruct managers on how to use the matrices. The roles and initial matrices were created based on input from focus groups consisting of subject matter experts from many federal agencies. The federal CIO Council's Information Security and Identity Management Committee (ISIMC) and ITWC advised on the project. Plans are underway to link the matrices to the Framework by providing sample illustrations of how the specialty areas within

the Framework can be mapped to create various cybersecurity roles.

The Framework is comprehensive and inherently flexible, allowing organizations to adapt its content to their human capital and workforce planning needs. The work conducted in the federal CIO Council's Cybersecurity Workforce Development Matrix project will be leveraged to provide government organizations with sample applications of how they can adjust the Framework to suit their own workforce needs. These sample applications provide an option for each department or agency to customize their template through the Framework model. Over time, these examples will be expanded to include the education, experience, credentials, and training needed by an individual for each role.

The Framework [9], published in August 2012, enabled the issuance of cybersecurity functional codes by OPM on October 1, 2012, in their "Guide to data standards" [16]. Use of these cybersecurity function codes will enable OPM and federal agencies to identify the cybersecurity workforce; determine baseline capabilities; examine hiring trends; identify skill gaps; and more effectively recruit, hire, train, develop and retain a valuable cybersecurity workforce.

An increased focus on the science of security at our nation's institutions of higher learning based on the R&D strategic plan's thrust of developing scientific foundations will produce graduates ready to enter the cybersecurity workforce with the skills to organize disparate areas of knowledge, leverage the universal laws to be discovered, and apply scientific method to their work. The National Cybersecurity Workforce Framework developers recognize that it will be vital for the workforce and science and technology communities to work together to acknowledge and communicate the importance of these skills and other newly discovered KSAs needed within our nation's workforce.

NICE end-state vision

Looking to the future, NICE envisions a developed workforce that is prepared to ensure an organized and unified response to cyber incidents. NICE envisions a nation that is prepared to work together to secure America's information and communications networks. Public-private partnerships, established to meet the NICE goals, will continue to collaborate to meet the demands of new threats and to utilize cutting-edge

R&D which is delivering the innovation and discovery that the nation needs to meet the challenges of our time. NICE envisions increased cybersecurity awareness from our boardrooms to our classrooms and a strong cybersecurity workforce for the twenty-first century. 

About the author

Bill Newhouse is a cybersecurity program lead in the Computer Security Division, one of six divisions in the Information Technology Laboratory at National Institute of Standards and Technology (NIST). Newhouse represents NIST in several collaborative efforts including (1) the National Initiative for Cybersecurity Education, (2) a partnership with the Department of Homeland Security and the financial sector to develop and test innovative cybersecurity technologies and processes, and (3) as a member of federal interagency cybersecurity R&D committees.

Before coming to NIST in 2010, Newhouse spent five years in the Office of the Secretary of Defense, where he focused on the cybersecurity and information assurance R&D portfolio, first with the assistant secretary of defense for research and engineering and then with the assistant secretary of defense for Networks and Information Integration (NII). While in NII, he championed Defense Venture Catalyst Initiative workshops to focus on cybersecurity solutions from innovative companies. He is an electrical engineering graduate of both the Georgia Institute of Technology and George Washington University and has been with the federal government for over 25 years, beginning as a cooperative education student at NSA in 1986.

References

- [1] The White House Office of the Press Secretary. "Remarks by the President on securing our nation's cyber infrastructure." 2009 May 29. Available at: <http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>
- [2] The White House. "Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure." Available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[3] To learn more about the National Initiative for Cybersecurity Education, visit <http://csrc.nist.gov/nice/>.

[4] To learn more about Stop.Think.Connect., visit <http://stopthinkconnect.org/>.

[5] To learn more about the National Cyber Awareness Coalition, visit <http://www.dhs.gov/stopthinkconnect-coalition>.

[6] To learn more about the Cyber Tours program, visit <http://stopthinkconnect.org/get-involved/homeland-security-campaign/cyber-tours-program>.

[7] To learn more about the Stop.Think.Connect. Toolkit, visit <http://www.dhs.gov/files/events/stop-think-connect-campaign-materials.shtm#1>.

[8] To learn more about the project to professionalize the nation's workforce, visit http://sites.nationalacademies.org/CSTB/CurrentProjects/CSTB_070783.

[9] To learn more about the National Cybersecurity Workforce Framework, visit <http://csrc.nist.gov/nice/framework/>

[10] Executive Office of the President National Science and Technology Council. "Trustworthy cyberspace: Strategic plan for the federal cybersecurity research and development program." 2011 Dec. Available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

[11] To learn more about common core state standards, visit <http://www.corestandards.org/>.

[12] National Governor's Association and Council of Chief State School Officers. "Common core state standards for mathematics." Available at: http://www.corestandards.org/assets/CCSSI_Math%20Standards.pdf

[13] To learn more about computational thinking, visit <http://www.cs.cmu.edu/~CompThink/>.

[14] To learn more about the Chief Information Officers Council, visit <http://www.cio.gov/>.

[15] Chief Information Officers Council. "Cybersecurity workforce development matrix resource guide." 2011 Oct. Available at: http://www.cio.gov/documents/Cybersecurity_Workforce_Development_Matrix_Resource_Guide_Oct_2011.pdf

[16] Office of Personnel Management. "Guide to data standards." 2012 Oct. 01. Page A-107. Available at: http://www.opm.gov/feddata/GDS/GDS_A09.pdf