In early 2010, the National Initiative for Cybersecurity Education (NICE) was created to help protect the nation from cyber threats by improving the cyber behavior, skills, and knowledge of the nation as a whole.

NICE was created with the idea that perhaps the most valuable resource in the fight against cyber threats is people: people who can create the technologies that protect information and resources, people who can recognize cyber threats and respond to them, and people who understand how to protect themselves in cyberspace.

The overall objective of the initiative is to create an operational, sustainable and continually improving cybersecurity education program that advances the long-term cybersecurity posture of the Nation.

Community Effort

Over the years, many disparate organizations from across industry, academia, and government have recognized a need and begun efforts improve the education or skills of cyber-technology users. Many of these efforts have unique target audiences, approaches, motivation and abilities. Some emphasize certifications, others promote new technologies, and still others focus on cyber ethics. While all are noteworthy efforts, it is difficult for an educator to determine exactly what it is they should be teaching. Because of this, some students emerge with inconsistent and unbalanced skill sets that may or may not benefit the job for which they are hired.

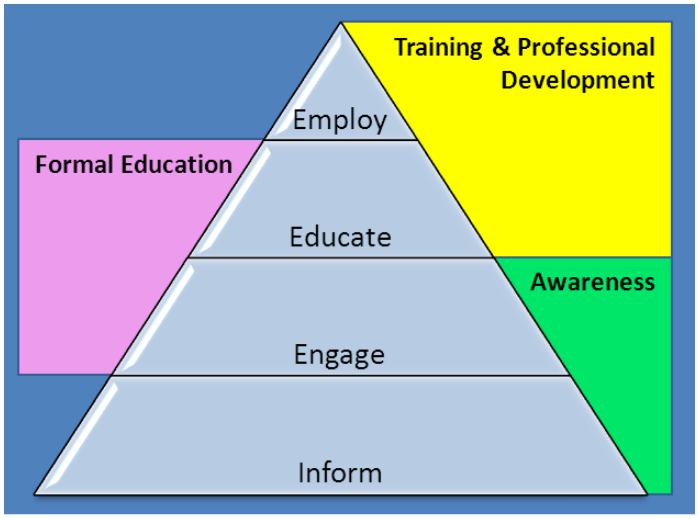
In cybersecurity, there is never a one-shot solution - no silver bullet – and cybersecurity education is no different. Right now, there is no single organization, method or program that can profoundly improve the cybersecurity education of the nation alone. Cyberspace's interconnected and distributed nature consistently demonstrates that a weakness at one point often has a profound impact on the security of another point. Because of this, NICE has been specially designed as a community effort, engaging academia, industry, government and public participation.

As the lead of NICE, National Institute of Standards and Technology (NIST) seeks to connect all of the existing cybersecurity education efforts together in order to help identify weaknesses or opportunities, share and expand strengths, and bring people together to solve lingering cybersecurity education problems.

NICE efforts have been divided into four complimentary components:

1. Awareness
2. Formal Education
3. Workforce Structure
4. Training and Professional Development

The Awareness, Formal Education, and Training and Professional Development components work together to cover the broad spectrum of cybersecurity education levels - from informing the public about how to avoid cybersecurity threats, to improving how cybersecurity skills are taught in schools, to training Federal cybersecurity professionals more effectively.



The Awareness, Formal Education, and Training and Professional Development components of NICE work together to cover the broad spectrum of cybersecurity education levels.

The Workforce Structure component provides a technical foundation for NICE by defining the cybersecurity workforce and creating a strategy for recruitment and retention.

Several Federal agencies have joined together with NIST to form the NICE team, including the Departments of Homeland Security, Education, Defense, Labor, Justice, Commerce, the National Science Foundation, the Office of Personnel Management, and the National Security Agency. In addition, a variety of academic, industry, and non-governmental organizations have become involved, sharing resources, lessons learned, and new ideas.

Workforce Framework

One of the more pressing problems that NICE has faced is the lack of consistency throughout the Federal government and the nation as to how cybersecurity work is defined or described. It is difficult to set job requirements, identify gaps, and provide training and professional development opportunities because of these inconsistencies.

In response, dozens of Federal government organizations, subject matter experts and industry partners have collaborated to create the NICE Cybersecurity Workforce Framework, available at http://csrc.nist.gov/nice/Framework. This draft document organizes cybersecurity work and workers into seven high-level categories and 31 Specialty Areas. The Specialty Areas each have a list of associated Tasks, Knowledge, Skills and Abilities (KSAs), and Competency areas.

The goal of this effort was to codify cybersecurity talent, to define the cybersecurity population in common terms and to tie the various jobs, occupations and responsibilities that require cyber skills together under a common architecture. Like the Periodic Table of elements, this Framework provides a structure and common lexicon for describing the cybersecurity workforce at its most basic levels. As such, it is intended to be comprehensive and to be compatible with all existing workforce models. It strives to capture every possible cybersecurity skill or competency (KSA) and sort them into every possible Specialty Area that relates to cybersecurity.

The Framework is also intended to be flexible. Organizations are free to select which Specialty Area skills and tasks (like the elements of the Periodic Table) apply to a specific work role. Similarly, as cybersecurity workers often play a number of roles in their organization and throughout their careers, workers can and should find themselves in more than one Specialty Area. For example, a System Administrator may conduct some of the tasks under System Administration and Knowledge Management, but doesn't use all of the KSAs in each Specialty Area.

This competency-based Framework expedites and gives rigor to workforce baselining, gap analysis, training catalogs, professional development resources, and more. Over the next few years, NICE will seek to validate the Framework, making any necessary changes, and encourage its adoption first in the Federal government and later in industry. However, its usefulness to academia is already apparent and crosses all levels of the education spectrum – from raising awareness to helping form curricula.

Inform & Engage

At the lower end of the education spectrum, the Framework can be used to get students interested in cybersecurity. Many don't realize the variety of cybersecurity fields, and many don't realize that they may already have many of the skills needed to perform a job function. For example, the Framework shows a worker performing in the Incident Response area may:

- Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
- Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents.

This may sound especially appealing to a student who otherwise would have shied away from the cybersecurity field. It shows how somebody in this Specialty Area could operate in the role of a detective, investigating incidents and then figuring out how to resolve them. Additionally, the Framework can be used to inform students and the public about how cybersecurity applies to more than just traditional Information Assurance fields. The Framework shows how cybersecurity skills and abilities are needed in a variety of jobs, including Legal Advisor, Contracting Officer, CIO, or Software Engineer.

Other students may find that they already have many of the KSAs for a Specialty Area. When looking at the list of KSAs under Vulnerability Assessment and Management, for example, a student could find they already have knowledge of data backups, basic system hardening techniques, and network architecture concepts. Thus, this Specialty Area and associated cybersecurity jobs may be especially appealing to that student. Having some or all of the KSAs for a Specialty Area gives students an idea of what sorts of positions they may enjoy and provide a solid foundation from which to build.

For educators looking to get students interested in cybersecurity, one great tool is competitions. The CyberPatriot National High School Cyber Defense Competition[1], Department of Defense Cyber Crime Center (DC3) Digital Forensics Challenge[2], National Collegiate Cyber Defense Competition (CCDC)[3], and other competitive arenas provide an exciting environment for students to learn about cybersecurity and gain hands-on experience. NICE has begun working to expand the use and usefulness of competitions in

[1] http://www.uscyberpatriot.org
[2] http://www.dc3.mil/challenge/
[3] http://www.nationalccdc.org/

cybersecurity education and relate them to the Framework. Often, students will find that the skills they use in cybersecurity competitions directly correspond to KSAs in one or more Specialty Areas.

Educate & Employ

Higher on the educational spectrum, the Framework can be used to bolster curricula and ensure students graduate with a useful set of skills. At this level, the Framework can be used to help answer these critical questions:

- What am I preparing my students for?
- What skills do they need?
- What should I be teaching?

By mapping existing curricula to the Framework and seeing which KSAs and Specialty Areas they cover, schools can better understand how their students are prepared for careers in cybersecurity. Each Specialty Area in the Framework can be viewed like a badge a student can wear. If they obtain the applicable KSAs and are trained on how to complete associated tasks, students can claim a badge (Specialty Area) and thus be better able to market themselves. When mapping curricula, it is important to take into account required and optional courses, within and outside of the Computer Science, Computer Engineering, or Information Assurance departments.

In some cases, schools may be surprised at how many or how few of the different Specialty Area KSAs are covered by their curriculum. Occasionally, schools may find that, while they expertly cover one or more competencies such as Computer Languages or Infrastructure design, these competencies only cover a small portion of cybersecurity work. Conversely, schools may find that their existing curricula, while not directed towards cybersecurity professions, cover many of the KSAs required.

The KSAs in the Framework often overlap and pull from several disciplines. Thus, identifying which skills students need to learn and how to teach those skills may not be an easy task. Many schools may choose to focus on the Specialty Areas, ensuring their students obtain all of the KSAs listed in a specific area. Others may allow the student to decide what career path they want and will select those courses that best cover the necessary KSAs. Many schools have relationships with industry partners. If these industry partners map their workforces to the Framework, they can help schools identify the cybersecurity skills they want in their employees, and schools can adjust their curricula accordingly.

Colleges and Universities looking to teach cybersecurity can use the Framework to help them qualify as a Center of Academic Excellence in Information Assurance Education (CAE/IAE)[4]. Gaining the CAE/IAE designation gives colleges and universities a prestige in the cybersecurity education sphere. Plus, students attending designated schools are eligible to apply for thousands of dollars in scholarships and grants through Federal and Department of Defense Information Assurance Scholarship Programs. By the

[4] http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

end of 2011, 118 academic institutions were designated as CAE/IAEs[5] and hundreds of scholarships and grants were awarded. The standards used by the Committee on National Security Systems (CNSS) to determine CAE/IAE qualification are currently being mapped to the NICE Framework, allowing schools to understand and describe their programs using a common lexicon and architecture.

If a school's curriculum needs to change in order to meet its cybersecurity education goals, this can be a simpler task than most realize. KSAs can be inserted into existing courses, or course requirements altered. There are many examples of how Information Assurance concepts can be integrated into seemingly unrelated topics such as Enterprise Architecture or Computer Language courses. For example, a basic networking course could be expanded to include information on IDS tools and applications. Software Development courses could include Information Assurance considerations. Or, a school could allow a Computer Science student interested in Digital Forensics to substitute a class on Computer Languages for a class on cyber law.

Each school will likely choose to structure and teach the KSAs differently. However it is done, correlating the Workforce Framework to a school's curriculum and ensuring all the appropriate KSAs are taught provides a way to help students more easily define and prepare themselves for a career in cybersecurity.

NICE also supports other great resources for educators, such as Advanced Technological Education (ATE) centers[6]. In these centers, community colleges, universities, secondary schools, industry, and government agencies work together to support curriculum development, professional development of college faculty and secondary school teachers, develop career pathways, and other related activities. Cyberwatch, The Center for System Security and Information Assurance, and the Cyber Security Education Consortium (SCEC) are some of the ATE programs that have proven extremely successful.

Get Involved

Improving the long-term cybersecurity posture of the Nation requires everybody's involvement. Besides the Framework, ATE centers, CAE/IAE, and other resources already mentioned, there are many other ways educators can help promote cybersecurity.

The National *Stop|Think|Connect* campaign[7] seeks to increase understanding among the general population about cyber threats and how to be more secure online. *Friends of the Campaign* is a consortium of individuals and organizations who help with the awareness campaign. Friends distribute campaign materials, blog about issues, and volunteer their time to help teach about cybersecurity issues.

Similarly, NICE has partnered with community centers, school districts, colleges and universities around the country to host Cyber Citizen Forums. Many parent, kids and university groups have successfully

[5] http://www.nsa.gov/public_info/press_room/2011/academic_excellence.shtml
[6] http://atecenters.org/
[7] http://www.dhs.gov/files/events/stop-think-connect.shtm

hosted Cyber Citizen Forums, teaching basic cybersecurity skills and prompting dialogue and action. Posters, banners, presentations and materials for hosting Cyber Citizen Forums are free to download and use[8].

The annual NICE Workshop, to be held in Fall 2012, provides a collaborative environment for educators to join with industry and government personnel to discuss important cybersecurity education issues, raise concerns, and discover new resources. Last year, over 300 attendees represented a broad array of organizations, from the University of Puerto Rico to the National Security Agency to the Microsoft Corporation. Topics discussed ranged from cybersecurity competitions to certifications to formalized curriculum.

Through these and other resources, NICE provides a pathway for industry, government, and academia to improve the cyber behavior, skills, and knowledge of the nation. Go to http://csrc.nist.gov/nice/ to find out more, and join in the conversation on Twitter by using the #nistnice and #cybersecurity hash-tags.

[8] http://www.dhs.gov/files/events/stop-think-connect-get-involved.shtm