Building Capacity for a Digital Nation

- Promote cyber-security risk awareness for all citizens;
- Build an education system that will enhance understanding of cybersecurity and allow the United States 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.

60-Day Cyber Review. The White House

National Initiative for Cybersecurity Education

NICE represents the evolution of the cybersecurity education component of the Comprehensive National Cybersecurity Initiative (CNCI), expanding it from a federal government focus to a larger **national** focus.

NICE was created to meet the cybersecurity training, education, and awareness priorities expressed in Chapter II, *Building Capacity for a Digital Nation,* of the President's Cyberspace Policy.

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.

The effort is for all U.S. citizens of all ages (pre-school to senior citizens), and all types of professions whether it be in academia (pre-school, K-12, college/universities), federal/state/local government, business (small medium to large size businesses/companies), or local community group or non-profit organization.

Upcoming Events

"Shaping the Future of Cybersecurity: Engaging Americans in Securing Cyberspace Workshop"

When: September 20-22, 2011

Where: NIST Main Campus, Gaithersburg, Maryland

Registration opening soon! Check the NICE website for more details.

Notice: NICE will present the National Initiative for Cybersecurity Education Strategic Plan in mid August for Public comments.

NICE Component Structure

As the designated lead, 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.

NICE activities build on the strong work of the Federal Agencies and Departments who are already focused on addressing cybersecurity training, education, and awareness needs. NICE begins its work structured to focus on four component areas.

Component 1: National Cybersecurity Awareness Campaign – goal to evolve improving behavior of the American public in cybersecurity. http://www.dhs.gov/files/events/stop-think-connect.shtm This component is lead by the Department of Homeland Security (DHS)

Component 2: Formal Cybersecurity Education – goal to broaden the pool of skilled workers for a cyber-secure nation. This component is being lead by the Department of Education and the National Science Foundation.

Component 3: Cybersecurity Workforce Structure – goal to define cybersecurity jobs, attraction, recruitment, retention, career path strategies. This component is being lead by DHS and supported by the Office of Personnel Management (OPM). This component contains the following Sub-Component Areas (SCAs):

- SCA1 – Federal Workforce: lead by OPM
- SCA2 – Government Workforce (non-Federal): lead by DHS
- SCA3 – Private Sector Workforce: lead by Small Business Administration, Department of Labor, and NIST.

Component 4: Cybersecurity Workforce Training and Development – goal to develop and maintain an unrivaled cyber workforce. This component is being lead by DHS, the Department of Defense (DoD) and the Office of the Director of National Intelligence (ODNI). This component contains the following Functional Areas (FAs):

- FA1 – General IT Use: lead by DHS and Department of the Navy
- FA2 – IT Infrastructure, Operations, Maintenance & Information Assurance: lead by DoD and DHS
- FA3 – Domestic Enforcement and Counterintelligence: lead by Defense Cyber Crime Center, Office of the National Counterintelligence Executive, Department of Justice, and United States Secret Service
- FA4 – Specialized Cybersecurity Operations: lead by the National Security Agency