NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) PROGRAM

NICE has evolved from the Comprehensive National Cybersecurity Initiative, and extends its scope beyond the federal workplace to include civilians and students in kindergarten through post-graduate school. The goals of NICE are to establish an operational, sustainable, and continually improving cybersecurity education, awareness, and training program for the nation and to increase the use of sound cyber practices which will enhance the nation's security.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) is leading the NICE initiative to ensure coordination, cooperation, focus, public engagement, technology transfer, and sustainability. Many NICE activities are already under way, and NIST will highlight these activities, engage various stakeholder groups, and create forums for sharing information and leveraging best practices. NIST will also be looking for "gaps" in the initiative -- areas of the overarching mission that are not addressed by ongoing activities.

NICE is organized into four Initiative Component Areas (ICAs):

ICA 1: National Cybersecurity Awareness

Lead: Department of Homeland Security (DHS)

The goal of ICA 1 is to boost national cybersecurity awareness. DHS will use public service campaigns to promote cybersecurity and responsible use of the Internet, and make cybersecurity a popular educational and career pursuit for older students.

ICA 2: Formal Cybersecurity Education

Co-Leads: Department of Education (DoED) and National Science Foundation (NSF)

The goal of ICA 2 is to bolster formal cybersecurity education programs encompassing kindergarten through 12th grade, higher education, and vocational programs, with a focus on the science, technology, engineering, and math disciplines to provide a pipeline of skilled workers for the private sector and government.

ICA 3: Cybersecurity Workforce Structure

Lead: Department of Homeland Security (DHS)

The Office of Personnel Management (OPM) is responsible for ICA 3 to ensure that federal agencies can attract, recruit, and retain cybersecurity employees. ICA 3 is divided into three Sub-Component Areas (SCAs):

SCA 1: Federal Workforce (Lead: OPM)

SCA 2: Government Workforce (nonfederal) (Lead: DHS)

SCA 3: Private Sector Workforce (Tri-Leads: NIST, Department of Labor, Small Business Administration)

ICA 4: Cybersecurity Workforce Training and Professional Development

Tri-Leads: Department of Defense (DoD), Office of the Director of National Intelligence (ODNI), Department of Homeland Security (DHS)

The goal of ICA 4 is to intensify training and professional development programs for the existing federal cybersecurity workforce. This ICA is divided into four Functional Areas (FAs):

FA 1: General IT Use (Co-Leads: DHS, Federal CIO Council)

FA 2: IT Infrastructure, Operations, Maintenance, and Information Assurance (Co-Leads: DoD, DHS)

FA 3: Domestic Law Enforcement and Counterintelligence (Lead: Department of Justice)

FA 4: Specialized Cybersecurity Operations (Lead: National Security Agency)

The Web site is: http://csrc.nist.gov/nice/.