National Institute for Cybersecurity Studies (NICS)
Ms. Peggy Maxson
29 March 2012
Agenda

• Background
• What is NICS?
• Components of NICS
  – Portal
  – Advisory Board
  – Virtual University
• NICS Timeline for 2012
• Call To Action
A National Problem

- The Nation needs greater cybersecurity awareness
- The US work force lacks cybersecurity experts
- Many cybersecurity training programs exist but lack consistency among programs
- Potential employees lack information about skills and abilities for cybersecurity jobs
- Resources exist for teachers and students about cybersecurity but are difficult to find
- Cybersecurity Career development and scholarships are available but uncoordinated
- Lack of communication between government, private industry, and academia

NICE was established to create a cybersecurity education program for the nation to use sound cyber practices that will enhance the nation’s security.
Four Components of NICE

NICE
NATIONAL INITIATIVE
FOR CYBERSECURITY EDUCATION

NATIONAL CYBERSECURITY AWARENESS
FORMAL CYBERSECURITY EDUCATION
CYBERSECURITY WORKFORCE STRUCTURE
CYBERSECURITY WORKFORCE TRAINING AND PROFESSIONAL DEVELOPMENT

NATIONAL INSTITUTE FOR CYBERSECURITY STUDIES (NICS)
NICS relationship to NICE

NICS was created to implement and share the resources and information produced by the four NICE components.
National Institute for Cybersecurity Studies (NICS)

NICS is a program that makes the awareness, education, training, and workforce development resources created by NICE available to the nation through a portal, an advisory board, and a virtual university.

NICS will:
- Focus cybersecurity education resources
- Influence the nation to become cyber aware
- Drive the pursuit of cyber careers

WEB PORTAL
Makes cybersecurity information and resources more readily available to the nation and promotes greater collaboration among cybersecurity students, educators, and employers.

ADVISORY BOARD
Comprised of representatives from government, academia, and industry, the advisory board provides recommendations to NICS for the development of cybersecurity awareness, education, and career training.

VIRTUAL UNIVERSITY
Enables Federal employees access to online training resources that are optimized for cybersecurity workforce development.
NICS Web Portal

The NICS Portal will be the main outlet of cybersecurity information and resources for the NICS program.
Find the Right Training

We've assembled training courses from hundreds of providers to create the most comprehensive listing of available Cybersecurity training. Courses are aligned to your career path. Find the training you need to enter the CS profession or advance your CS career:

Search 3,000+ Courses

Professional Certifications

A variety of professional certifications are available. View a list of certifications, learn their purpose and how to obtain them [Learn More].

FedVTE

Federal employees can access a rich library of cybersecurity and information assurance training. Put yourself in the classroom to attend lectures, work on demonstrations, and conduct hands-on labs. View and manage your organization’s workforce as they progress toward their training objectives [Learn More].

Workforce Framework

Experts across the country have begun the professionalization of the Cybersecurity domain. The first step in this effort was the development of a professional taxonomy that identifies and categorizes areas of the Cybersecurity discipline.

At this time each area has been mapped to the Federal, Office of Personnel Management (OPM), Knowledge, Skills, and Abilities (KSAs). We are seeking the input of commercial industry to further develop the framework [Learn More].

Training Spotlight on UMUC

University of Maryland University College (UMUC) has been an active leader in developing Cybersecurity curriculum and enhancing the Cybersecurity profession. Educators at UMUC have been actively involved in the Workforce Framework effort and were among the first to map their courses to the KSAs.

Engaging Courses, Varied Offerings

From basic introductory classes to extensive, hands-on experience in Digital Forensic techniques, UMUC offers a broad spectrum of CS courses and CS degrees. Their curriculum includes undergraduate and graduate degrees with a focus on career professionals looking to expand their expertise. Students may select from traditional classroom experience or dynamic online environments ideal for the working professional [Learn More].

About UMUC

Founded in 1947, UMUC is one of 11 accredited, degree-granting institutions in the University System of Maryland (USM). Offering a broad range of online graduate degrees, UMUC has earned a global reputation for excellence as a comprehensive virtual university. Its faculty and professional staff are dedicated to the success of its unique, self-paced and student-centered learners. UMUC serves students worldwide. Learn More [Learn More].
User and Subject Matter Expert Outreach

• Conducted user testing at NIST Workshop in September 2011
  – Total of 61 participants
    • 26 Educators
    • 15 Government Officials
    • 10 Workforce Professionals
    • 2 Students
    • 8 Other
  – Used 215 Scenarios to identify design concerns such as navigation and layout and conceptual issues such as the purpose of and the audience of the NICS portal.

• Conducted WebEX Sessions in January & February 2012
  – Held 4 sessions to gather feedback on the operation and content of the Portal
    • Content Vetting
    • Education
    • Training
    • Workforce Development
NICS Advisory Board

An advisory board composed of stakeholders with training and education focus from each of the target sectors will guide:

• Identification of cybersecurity best practices

• Identification of gaps and strategies for national cybersecurity training and professional development

• Academic institutions in addressing cybersecurity education needs based on skills sought in current cybersecurity environment
Virtual University

NICS Virtual University

• Federal employees access online cybersecurity training

• Link to Federal Virtual Training Environment (FedVTE)

• Access to a database of 160 brick and mortar facilities providing classroom training opportunities

• Future plans expand the online training to State Local Tribal Virtual Training Environment (SLTVTE)

• Link to the Federal Cybersecurity Training Exercise (FedCTE) platform
What Are the Current NICS Activities for FY 2012?

**NICS Portal:** Launch portal that serves as the nation’s online resource for government, industry, academia and the general public to learn about cybersecurity awareness, education, careers and workforce development opportunities.

*Key Activities*: Design Portal (Mar 2012), Focus Groups for Portal (Apr 2012), and Launch Portal Phase I (Sep 2012)

**Project Management Office:** Establish a Project Management Office (PMO) which will manage, support and maintain the NICS portal.

*Key Activities*: Develop PMO Operational Documents (Jun 2012), Acquire PMO Resources (Aug 2012), and Establish PMO (Sep 2012)

**Advisory Board:** Establish an Advisory Board to provide guidance, recommendations, and best practices on cybersecurity awareness, education, careers, and training programs.

*Key Activities*: Identify Advisory Board Tasks (Apr 2012), Identify Portal Advisory Board Members (Jun 2012), and Convene Advisory Board (Sep 2012)

*Dates are subject to change based on availability of funding and resources.*
Call To Action

Please use the NICS mailbox NICS@hq.dhs.gov to:

• Provide general comments or feedback on the Portal.

• Provide suggestions for additional material that should be included on the portal.

• Provide suggestions for Advisory Board members.

• Join our focus groups!
Do you want to help us define the cybersecurity field? Are you interested in participating in a Focus Group?

<table>
<thead>
<tr>
<th>Session Date/Time</th>
<th>Participant Requirements</th>
</tr>
</thead>
</table>
| Tuesday, April 10th, 10:00am-12:00pm | Mid/Seasoned Federal Government Professionals & Cybersecurity Trainers  
• 7+ years working in Cybersecurity field or as a Trainer for cyber  
• Federal Government career focus |
| Thursday, April 12th, 10:00am-12:00pm | Early Career Professionals & Cybersecurity Recruiters  
• 1-5 years working in Cybersecurity field or as a Recruiter for cyber  
• Federal or Private Industry/Commercial career focus |
| Tuesday, April 17th, 10:00am-12:00pm | Mid/Seasoned Industry Professionals & Cybersecurity Trainers  
• 7+ years working in Cybersecurity field or as a Trainer for cyber  
• Private Industry/Commercial career focus |
| Thursday, April 19th, 10:00am-12:00pm | Educators/Administrators in Cybersecurity Academia  
• 5+ years working in Cybersecurity with grades P-12  
• Cybersecurity education career focus |

Contact Peggy Maxson: Margaret.Maxson@hq.dhs.gov; 703-235-3654