

CNCI Education Initiative Status

Presented by:

Brenda Oldfield

Director, NCSD/CEWD

DHS Lead: CNCI Education Initiative

March 23, 2010



Homeland
Security

OBJECTIVE:

Provide the USG with a technically adept cyber workforce capable of achieving the goals of the CNCI.

With an initial focus on *role-based, specialized skills* of the *current cyber personnel* and the *pipeline of future cyber recruits*, this effort will expand the capabilities of today's workforce and prepare the future USG workforce.



CNCI Cybersecurity Education Status

- **Education Initiative Senior Steering Committee** - collaborative interagency working group assigned from civilian, intelligence, defense and law enforcement agencies.
- **Cybersecurity Education Partnerships** - DHS to accomplish its CNCI responsibility via interagency agreements with the agencies with official responsibility and/or operational infrastructure in place to initiate and implement targeted activities.

INTERAGENCY SENIOR STEERING COMMITTEE

DHS & DoD/NSA, Co-Leads

DOS: DS, FSI

DHS: NCSA

DOC: NIST

DOD: NSA, DIAP, DC3

DOJ: FBI

ODNI: ONCIX

NSF



Strategy Addresses 3 Drivers:

- 1) Develop a framework for career development in cybersecurity that keeps pace with technological change
- 2) Create a systematic approach and common taxonomy of cybersecurity skill sets and standards
- 1) Accelerate the availability of skilled workers in the Federal pipeline



COMING TO A PC NEAR YOU -- SUMMER 2010 !!!!!!!

- ✓ **IT Security Courseware and Hands-on Labs, via Virtual Training Environment (VTE)**
- ✓ **Federal Cybersecurity Training Exercise Program**



**Homeland
Security**

Keep pace with technological change

Government-wide Access to Virtual Training Environment (VTE)

Deploy online, on-demand training content to Federal IT Security users (> 800 hours of role-based skills training and hands-on laboratories)

- Role-based skills training
- Hands-on laboratories
- Will Support >100K Federal IT security users
- ~20K simultaneous users
- Access entirely via web-browser

Department of State, Foreign Service Institute:

Initial setup of hosting environment and support; acquire hardware/software; C&A of platform & facility

Carnegie Mellon University/Software Engineering Institute (CMU/SEI):

Deliver technical and operating specifications; application and content transfer; and instructor support



Federal Cybersecurity Training Exercise Program

- Develop a framework, design model to provide attack/defend training exercises for civilian agency staff
- Conduct pilot sessions using both simulations & virtual labs for active-learning experiences
- Evaluate results/make recommendations for full implementation
- Scope for national expansion - State/Local government

Cybersecurity Education Partnership

DHS/ Department of State-Diplomatic Security Training Center



Homeland
Security

Keep pace with technological change

vGOV

Trusted Source Hosting Project

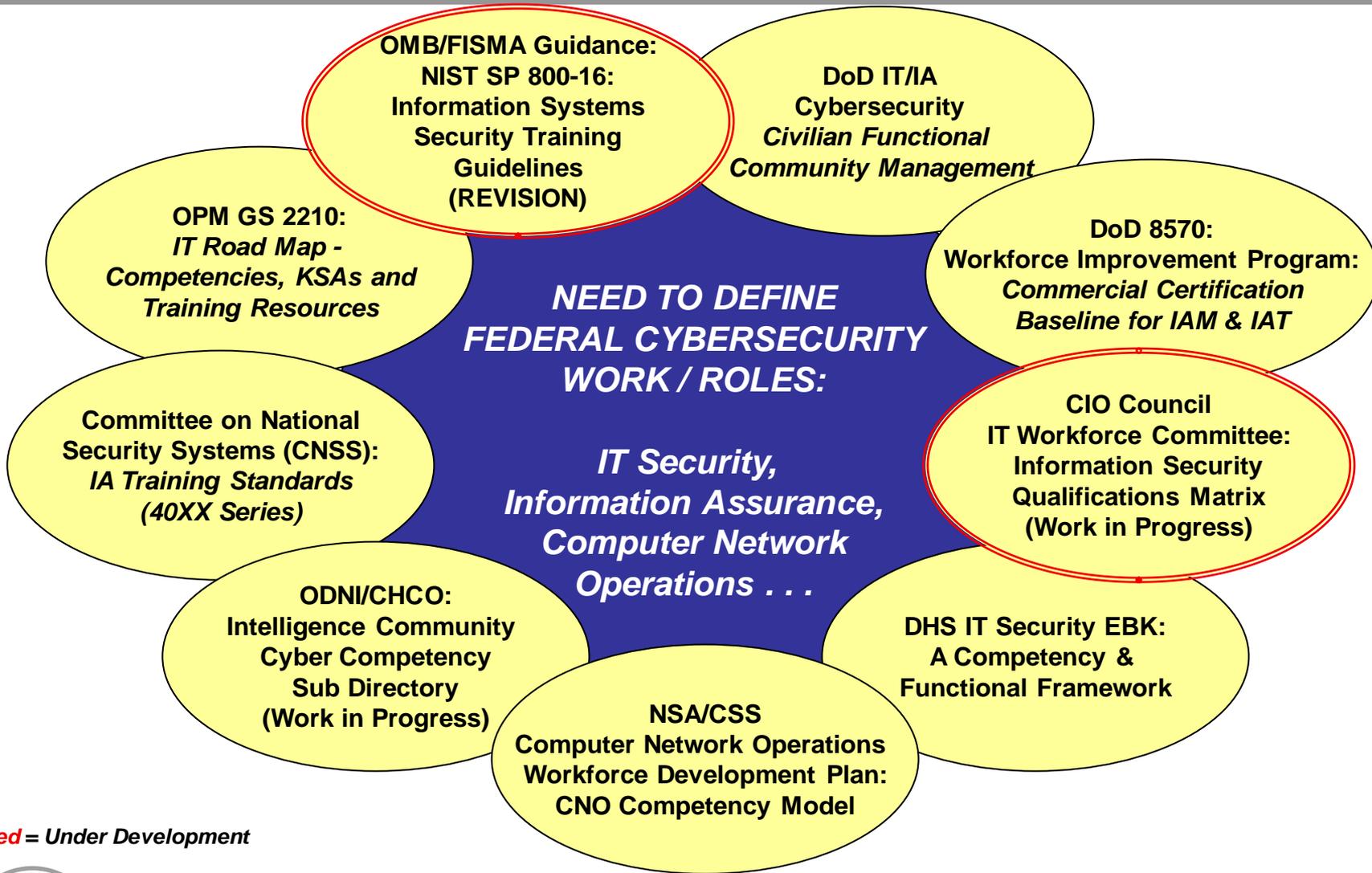
- Federal Virtual Worlds Consortium partnership: USDA & NDU-IRM College
- Promote collaboration and an interchange of expertise
- Government-wide, multi-agency secure access to virtual worlds content repository
- Develop prototype user cases for cybersecurity training

Outcome:

Proof of concept, secure environment for cybersecurity training



Federal 'Cybersecurity' Skills Qualifications & Training Requirements/Standards



Red = Under Development



Homeland
Security

Create a systematic approach

Federal Cybersecurity Competency Synchronization Activity

- Review existing cross-community IT security, information assurance, information security training guidelines/standards
- Compare & contrast “cybersecurity” efforts currently underway in civilian, IC, and defense agencies
- Determine how current federal titles, work roles, job definitions, & training activities map to the concept of “cybersecurity”

OUTCOME:

A flexible taxonomy of cybersecurity functions, competencies, & work activities that are typical across government



Federal Cyber Service and National Centers of Academic Excellence in IA Education Programs

Establish and implement 2YRCAE Community College program

✓ 1st 6 schools designated, March 2010

Sponsored International Review of IA Curricular Standards

✓ Report published to ACM/IEEE website, December 2009

Develop CAE model for education, training and academic outreach in support of cybersecurity of the critical infrastructures

✓ Academic WG established

Annual co-sponsorship: CAE/IAE and SFS programs

Implement SFS Mentorship Facilitation Pilot



Software Assurance (SwA) Education & Training Products

Load SwA curriculum content & training tools to the CMU/SEI Virtual Training Environment for wide dissemination to colleges/universities



- ✓ **Colloquium of Information System Security Educators (CISSE)**
- ✓ **2010 National Collegiate Cyber Defense Competition (NCCDC) and Regional CCDC Competitions**
- ✓ **Federal Information System Security Educators Association (FISSEA)**
- ✓ **Digital Forensics Educators Working Group (with FBI)**
- ✓ **State Government Information Security Workforce Development Model**

