Introducing . . .

Sponsored by:

Cybersecurity Education Office (CEO)
DHS National Cyber Security Division

FISSEA 2011
Coming to a PC near you!

Federal Virtual Training Environment (FedVTE)  Federal Cybersecurity Training Events (FedCTE)

2011
NSPD-54/HSPD-23
Education Initiative

Senior Steering Committee - civilian, intelligence, defense, law enforcement

DHS/Department of State Cybersecurity Training Partnerships:
- Foreign Service Institute – FedVTE
- Diplomatic Security Training Center - FedCTE

Drivers/Objectives:
- Develop a framework for cybersecurity training/career development that keeps pace with technological change
- Focus on role-based, specialized skills of current cybersecurity personnel to expand the capabilities of today’s workforce
2-programs developed in parallel
To supplement role-based Federal IT security training
Audience
Personnel who protect U.S. Federal information & IT systems
IPv4 to IPv6 Transition: Mechanisms

Dual IP Stack Operating Systems and Applications

IP Tunnels

Translation Gateways

Takeaways

IPv4 Disable - DoD Definition

Navigation

Demo
IPv6 Transition Options
IPv4 to IPv6 Transition: Mechanisms
Transition Issues
FedVTE Development

2011

Pilot test

Spring

System operational

Winter

Transition existing users

Summer

Open enrollment

400+ volunteers; 40+ departments & agencies
Cybersecurity Training Events
Interactive, experiential training for Federal cybersecurity workforce
FedCTE Program Development

Operation Cyber Threat (OCT)

- 3 events in 6 months
- Mixture of collocated & distributed
- 98 students
- 41 agencies
- 38 cities

See DSTC information booth in the lobby for information on upcoming events
Here’s how it works

POC = department/agency point of contact
TA = department/agency Training Advisor

Certificates
Usage Reports
Homework

Help us establish POCs and TAs at your Department or Agency.

- CIO or CISO must nominate a POC
  - Nomination email should be sent to FedVTE@dhs.gov
  - Include POCs full name and email address

- Get organized! Establish TAs who can…
  - Identify IT security personnel
  - Authorize training for personnel
  - Run reports