IDA

Institute for Defense Analyses
4850 Mark Center Drive • Alexandria, Virginia 22311-1882

Customize the Message to the Audience

A Dialogue about the Strategy for Awareness, Education, and Training related to Cybersecurity's Newest Threat – Global ICT Supply Chain Exploitation

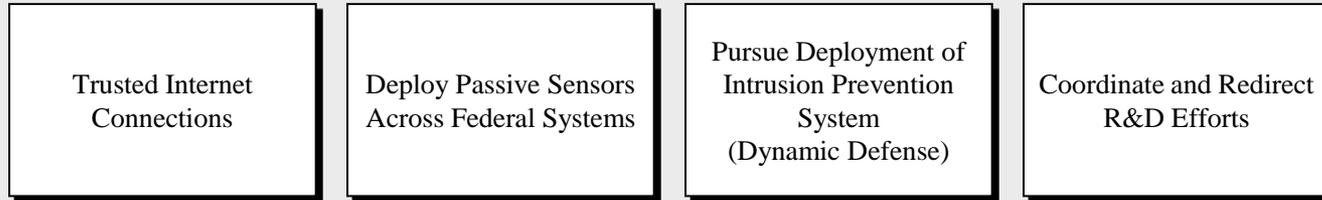Elizabeth A. McDaniel
Thomas Barth
Institute for Defense Analyses

FISSEA Annual Conference
March 21, 2013
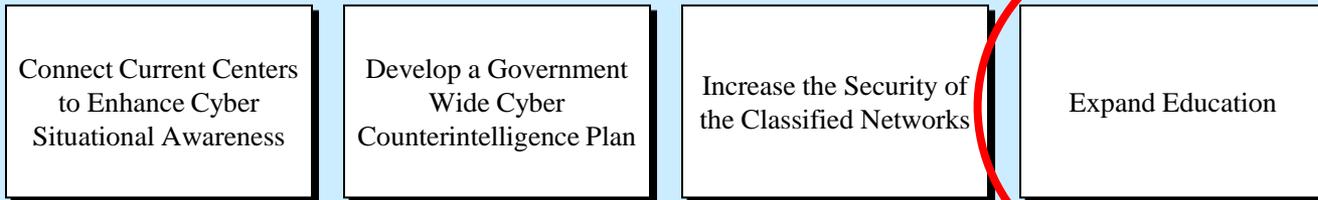
What is the Global Supply Chain?

Comprehensive National Cybersecurity Initiative (CNCI)

IDA

Focus Area 1

- Trusted Internet Connections
- Deploy Passive Sensors Across Federal Systems
- Pursue Deployment of Intrusion Prevention System (Dynamic Defense)
- Coordinate and Redirect R&D Efforts

Establish a front line of defense

Focus Area 2

- Connect Current Centers to Enhance Cyber Situational Awareness
- Develop a Government Wide Cyber Counterintelligence Plan
- Increase the Security of the Classified Networks
- Expand Education → NICE

Demonstrate resolve to secure U.S. cyberspace & set conditions for long-term success

Focus Area 3

- Define and Develop Enduring Leap Ahead Technology, Strategies & Programs
- Define and Develop Enduring Deterrence Strategies & Programs
- Develop Multi-Pronged Approach for Global Supply Chain Risk Management
- Define the Federal Role for Extending Cybersecurity into Critical Infrastructure Domains

Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors

Core Content of Global ICT SC Exploitation and Risk Management

National Security Issues & Drivers	Global ICT SCRM Basics	Criticality Analysis	Threat Analysis	Vulnerability Analysis	Impact	Managing the Taking of Risks	Mitigation and Counter-measures	Performance, Cost and Schedule Trade-offs