CIO/NII Enabling Net-Centric Operations

DoD Shared Service Center for Security Awareness Training

Cathy Fillare, OSD DIAP
Maryann Dennehy, DISA FSO
Bryan Lakey, DISA FSO
7 March 2007

CIO/NII Enabling Net-Centric Operations

DoD's Model for the Security Awareness SSC

- Leverage current DoD IA Awareness baseline product
- Centralized awareness product development
- Decentralized awareness program implementation
  - Delivery via web-based training and CBT
  - Tracking via customer specific LMS/mechanisms
  - Reporting via customer specific LMS/mechanisms
- Target audience is DoD Components and Departments and Agencies with National Security Systems

CIO/NII Enabling Net-Centric Operations

DoD SSC Roles and Responsibilities

- Office of the Secretary of Defense (OSD) responsible for business administration
  - Prepare Service Level Agreements
  - Facilitate funding of unique content/features
  - Integrate with other Awareness SSC's
- Defense Information Systems Agency (DISA) responsible for product development
  - Collect requirements
  - Develop and manage content
  - Deliver product for customer implementation

CIO/NII Enabling Net-Centric Operations

DoD IA Awareness Baseline Development

- Web-based product to meet requirements of:
  - FISMA/OMB ISS LOB
  - DoD 8570.01-M
  - Other, as agreed upon by DoD Components
- Requirements collaboration under auspices of DoD IA Workforce Improvement Program Advisory Council
- No cost to DoD Components, Federal Departments and Agencies for baseline product
  - Does not include DoD Component, Federal Department or Agency specific content

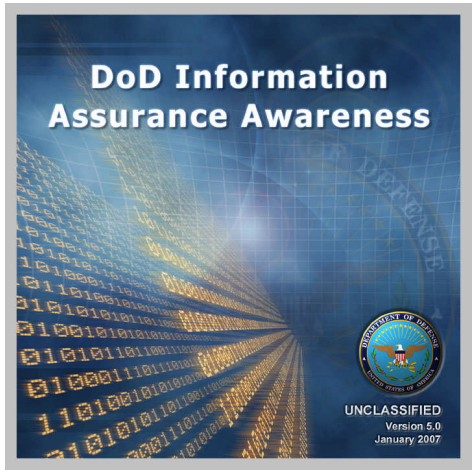
CIO/NII Enabling Net-Centric Operations

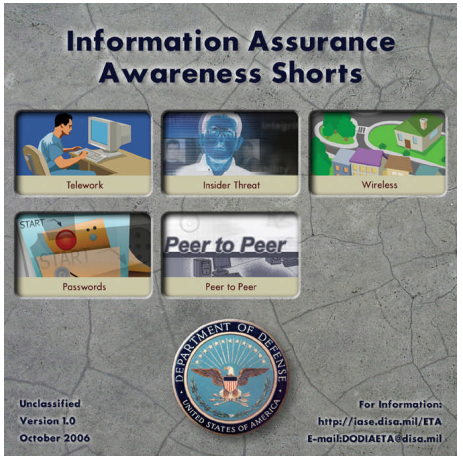
DISA Information Assurance (IA) Education, Training & Awareness (ETA) Program Overview

- Created in early 1990s to address need for department-wide IA education, training, and awareness in the DoD
- DISA IA training products are developed in a distributive, multimedia format for a globally-dispersed audience of over 2 million DoD military, civilian personnel, and contractors
- DISA's *award-winning* IA training products are widely-distributed to U.S. government at federal, state, and local levels, as well as to high-level military and civilian academic institutions, international allies, and coalition partners
- DISA IA training products are used to support DoD IA professionalization and user certification objectives for system administrators, information assurance officers and managers (IAO, IAM), designated approving authorities (DAA), and other IA personnel, as well as DoD user awareness training requirements

DoD IA Training Products

- Support certification of DoD IA professionals
- Compliant with Section 508 of the Rehabilitation Act
- Mapped to:
  - CNSS Training Standards
  - DoD 8570.01-M
    - *Includes all 800-50 end user awareness requirements*
  - NIST SP 800-16
- Available at no cost ***(http://IASE.DISA.mil/eta)***

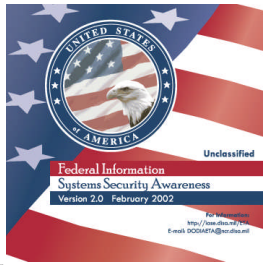




DoD IA Training Products, Cont'd

- Adapted by other DoD organizations
  - USN, USMC, Army, USAF, NDU

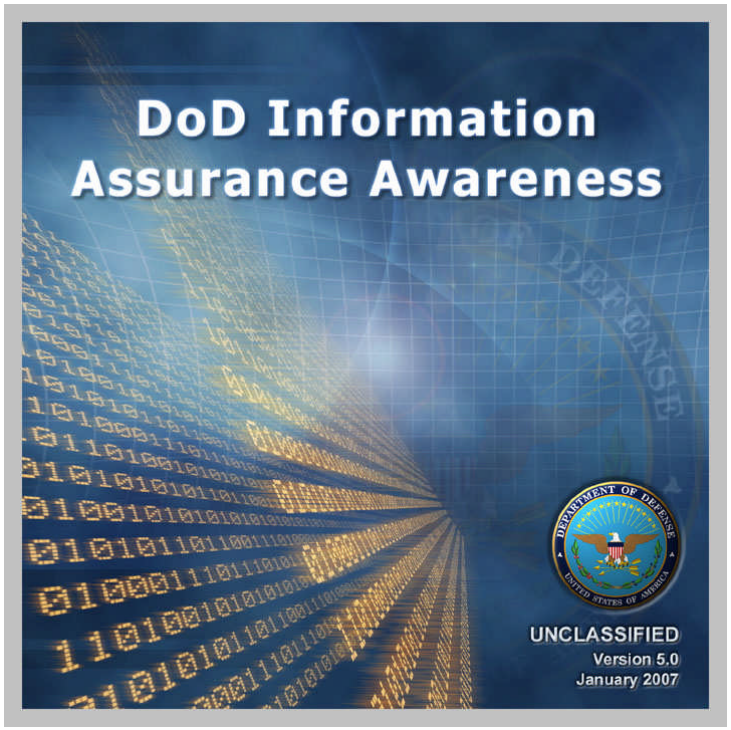
- Tailored by other Federal agencies
  - Federal Information Systems Security Awareness
    - Sponsored by FISSEA
  - Dept of State
  - Dept of Treasury
  - HHS
  - DOE
  - NASA



Demos

Ease of Use
Completeness
Technical

- **DEMO: DoD IA Awareness**



CIO/NII Enabling Net-Centric Operations

Importance of Information Assurance

- IA Overview
  - IA Publicity
  - IA Defined (CIA)
- Evolution of IA
  - History of IA
- Policy and Law
  - IA Legal Requirements (FISMA, OMB Circular A-130)
  - DoD Policy Documents (DoDD 8500.1, DoDI 8500.2, C&A)
  - DISN (NIPRNet, SIPRNet)
- Critical Infrastructure Protection

CIO/NII Enabling Net-Centric Operations

Threats to Information Assurance

- Threats and Vulnerabilities
  - Threats vs. Vulnerabilities Comparison (Definitions, IAVM)
  - Threat Categories (Human, Natural)
  - Internal vs. External Threats
- Social Engineering
  - Social Engineering Overview
  - Your Role in Social Engineering (Preventing, Reacting)
  - Example
- Internet Security
  - Cookies
  - Mobile Code
  - Mobile Code Categories
  - DDoS
  - P2P

CIO/NII Enabling Net-Centric Operations

Malicious Code

- Malicious Code Overview
  - What is Malicious Code?
  - E-mail and Attachments
- Protecting Your System
  - Preventing Malicious Code
  - Reacting to Malicious Code
- Understanding Internet Hoaxes
  - Hoaxes
  - What to do when receiving Hoax

CIO/NII Enabling Net-Centric Operations

User Roles and Responsibilities

- System Security
  - Basic User Guidelines (Monitoring, Computer Misuse)
  - PKI (CAC)
  - Secure Passwords
  - INFOCONs
- Protecting DoD Information
  - Backups, Storage, and Labeling
  - Securing Media Devices (Phone, Cell, Laptop, PDA, Wireless)
  - Data Classification (Classified, Unclassified)
  - Spillage
  - PII
  - Your Responsibility

CIO/NII Enabling Net-Centric Operations

Personal and Home Computer Security

- Online Transactions
  - Identity Theft
  - Spyware
  - Phishing
  - Telework Procedures and Guidelines
  - E-Commerce
- Security Tips
  - Basic Security Principles (Use Antivirus Software, Scan Attachments, Apply Patches, Use Firewall, Make Backups, Select good Passwords, No P2P)
  - Technology

CIO/NII Enabling Net-Centric Operations

IA Awareness Update process

- Updated semi-annually
- Next update – July 2007
- Topics for inclusion vetted through the WIPIC sub-working group titled “DoD IA Training Advisory Working Group (DTAWG)”
- Audience: Basic users - not geared to technical or IA professionals
- DoD focused - not service/agency specific
- Addresses security awareness training requirements identified in:
  - ISS LOB
  - DoD 8570.01-M
  - CJCSM 6510.01
  - FISMA

CIO/NII Enabling Net-Centric Operations

Delivery Mechanism

- CD-ROM
- Web-based
- LMS implementation
  - DISA provide SCORM conformant CD
  - DISA provide limited support for organizations LMS implementation

CIO/NII Enabling Net-Centric Operations

Reporting

- Each agency manages their own FISMA reporting requirements

CIO/NII
Enabling Net-Centric Operations

Tailor it for your Organization

- Request quote through DoDAwarenessLOB@osd.mil

CIO/NII Enabling Net-Centric Operations

Questions

- Email DoDAwarenessLOB@osd.mil for more information

- POC
  - DoD: Catherine.Fillare.ctr@osd.mil
  - DISA: Maryann.Dennehy@disa.mil
  - SAIC: lakeyb@saic.com