fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's New in Cyber Security Training?

Susan Hansche

GovSec 2008– Washington, DC

Nortel Government Solutions

April 23, 2008

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

Cyber Security and Training

Ms. Susan Hansche, CISSP-ISSEP, CISM is the Program Director (Nortel Government Solutions) for the Role Based Information Assurance (IA) Training Program at the U.S. Department of State.

In addition, she is the author of the "Official $(ISC)^2$ Guide to the ISSEP CBK (2006) and is lead author of the "The Official $(ISC)^2$ Guide to the CISSP Exam" (2004).

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

Cyber Security and Training

- What's New?
  - Federal Regulations and Initiatives
  - Federal Cyber Security Training
- What's Important?
  - Identifying Employees with Significant Information Security Responsibilities
  - Standardized, baseline training curricula

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's New

Federal Regulations and Initiatives

What's New?
Federal Regulations and Initiatives

FISMA of 2002
H. R. 2458, Title III Information Security

Federal Agency Responsibilities:

"(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities"

What's New?
Federal Regulations and Initiatives

OPM 5 CFR part 930, subpart C
Training Requirement

- Each Executive Agency must develop a plan for Federal information systems security awareness and training
- Identify employees with significant information security responsibilities and provide role-specific training

What's New?
Federal Regulations and Initiatives

NIST SP 800-53 Awareness & Training (AT) Control

- AT1 (Policy): The organization develops, disseminates, and periodically reviews/updates: (i) a **formal, documented, security awareness and training policy** that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

What's New?
Federal Regulations and Initiatives

NIST SP 800-53 Awareness & Training (AT) Control

- AT2 (Awareness): **The organization provides basic security awareness training to all information system users** (including managers and senior executives) before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency, at least annually*] thereafter.

What's New?
Federal Regulations and Initiatives

NIST SP 800-53 Awareness & Training (AT) Control

- AT3 (Training): The **organization identifies personnel that have significant information system security roles and responsibilities** during the system development life cycle, documents those roles and responsibilities, and **provides appropriate information system security training:** (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.

What's New?
Federal Regulations and Initiatives

NIST SP 800-53 Awareness & Training (AT) Control

- AT4 (Record Keeping): The organization **documents and monitors** individual information system security training activities including basic security awareness training and specific information system security training.

What's New?
Federal Regulations and Initiatives

NIST SP 800-53 Awareness & Training (AT) Control

- AT5 (Outreach): The organization **establishes and maintains contacts** with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's New?
Federal Regulations and Initiatives

Information Sharing

The efficient interchange of information between agencies and appropriate state and local governments.

The Global Justice Information Sharing Initiative (Global) states that "information sharing is at the very heart of modern public safety and law enforcement."

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's New?
Federal Regulations and Initiatives

- Federal Desktop Core Configuration (FDCC)
  - OMB-mandated security configuration.
  - The FDCC currently exists for Microsoft Windows Vista and XP operating system software.
  - www.fdcc.nist.gov
- Security Content Automation Protocol (SCAP)
  - NIST established a suite of interoperable and automatable security standards
  - National Vulnerability Database
  - www.nvd.nist.gov

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's New?
Federal Regulations and Initiatives

Streamline Computer System Infrastructure Across Government

IT Consolidation

- Performance measurements will be established first in desktop computer management.
- This will be followed by metrics for data centers and for networks.
- The initiative also will promote the sharing of information and best practices, and the leveraging of aggregate purchases.

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's New?
Federal Regulations and Initiatives

IT Consolidation

- Advantages
  - Potential cost savings
  - Federal mandates
  - Ability to reduce redundancies
  - Ability to reduce vulnerabilities and manage risks
- Disadvantages
  - Loss of control
  - Slow application or poor performance
  - Single point of failure

What's New?
Federal Regulations and Initiatives

GARTNER GROUP Report

"But with a potential business downturn ahead for many clients, the next most important business value action to take will be to cut IT costs."

http://www.gartner.com/it/themes/optimize/optimize.jsp?ref=4_14_08RR

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's New

Federal Cyber Security Training

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's New?
Federal Cyber Security Training

- Information System Security Line of Business (ISS LOB)
  - Tier 1 Awareness
    - 3 choices – OPM, DoD, and JSAS (Joint State Dept/US AID)
  - Tier 2 Training
    - Planning Stage

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's Important

Identifying Employees with Significant Information Security Responsibilities

Standardized, baseline training curricula

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's Important?

Identifying Employees with Significant Information Security Responsibilities

- What methodology is needed in order to identify the personnel (and positions) with significant information security responsibilities?
- Who should validate the list?
- Should there be a "federal standard" that identifies personnel?

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

What's Important?

Standardized, Baseline Training Curricula

- Is it possible?
  - Basic System Examples: Comptia A+, Network+
  - Impact of FDCC
  - CNSS Guidelines, NIST Guidelines, OPM Competencies, DHS EBK
- Do the agencies want it?

What's Important?

What makes training good?

- Goal-oriented
- Takes advantage of existing knowledge
- Relevant and practical
- The participants are involved
- Transference exercises

http://www.csc.noaa.gov/training/facilities/

Hands-on computer exercises, real-life case studies, and group exercises

fissea
Federal Information Systems Security Educators' Association
AWARENESS • EDUCATION • TRAINING

Cyber Security Training

Susan Hansche

(571) 226-9480

susan.hansche@nortelgov.com