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

www.fissea.org

Identifying Employees with Significant Security Responsibilities: According to Who?

Susan Hansche

FISSEA Conference 2008

March 13, 2008

NIST, Gaithersburg, MD

FISMA Says . . .

- The head of each agency shall . . . delegate to the agency Chief Information Officer . . . training and overseeing personnel with ***significant responsibilities for information security*** . . .
- The head of each agency shall . . . ensure that the agency has trained personnel sufficient to assist the agency with complying with . . .

FISMA: Train People with Significant Responsibilities . .

- How to Decide?
- Where should it be documented?
  - Policy?
  - Position Descriptions?
  - Performance or Security Plans?
  - Contingency Plans, COOPs?
  - IG Reports? (Wait for IG Report?)
- Just Makes Sense?
- Good Security Practice? (Get Buy-in)

OPM CFR 930.301 (1997, updated 6/2004) Says . . .

- Develop awareness and training plan
- All users of federal information systems must be exposed to awareness materials at least annually
- **Identify employees with significant information security responsibilities** and provide role-specific training in accordance with NIST standards and guidance

OPM CFR 930.301 Also Says . . . Agencies Must Train . . .

- Executives
- Program and functional managers
- CIOs, IT security program managers, auditors, and other security oriented personnel (e.g., system and network administrators, and system/ application security officers)
- IT function management and operations personnel

NIST Guidance

- Updating NIST SP 800-16
- Looking at Job Functions
  - Primary consideration
  - Secondary consideration
- Will be vetted through public review and comment period(s) -- and possibly workshops

Employees with Significant Information Responsibilities

- Who?
  - CIO?
  - CISO & Security Staff?
  - System Owners?
  - Application Owners?
  - Data Owners?
  - Contractors?

Employees with Significant Information Responsibilities

- Who?
  - Network Administrators?
  - System Administrators?
  - Server (e.g., mail, web) Administrators?
  - Records Management Officials?
  - Law Enforcement Officials?
  - General Counsel?

fissea

What's the goal?

- Right people with the right skills are in the right place at the right time
- Get an A on FISMA score card

Ideas, Thoughts, and Experiences

Discussion Topics

- 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?

THANK YOU!

Contact Information

Susan Hansche, CISSP/ISSEP

Nortel Government Solutions

Program Manager for Department of State
IA Training Program

(571) 226-9480

Susan.hansche@nortelgov.com