Federal Information Security Management Act of 2002

Presentation to the

2003 FISSEA Conference

March 4, 2003

Federal Agency Responsibilities in FISMA

- The head of the agency delegates to the CIO (or comparable official in an agency without a CIO) a number of information security responsibilities. The CIO in turn designates a senior agency information security officer.

Professional Qualifications of the Senior Agency Information Security Officer

- The Senior Agency Information Security Officer shall:

  “possess professional qualifications, including training and experience, required to administer the functions described under this section”

Functions of the Senior Agency Security Official

The Senior Agency Security Official is responsible for:

- Developing and maintaining an agency wide information security program
- Developing and maintaining information security policies, procedures and control techniques
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities
- Assisting senior agency officials concerning their responsibilities

Responsibilities of the Head of the Agency (partial list)

- Ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards and guidelines; and
- Ensure that the agency CIO in coordination with other senior agency officials reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

Training Aspects of an Agency Wide Information Security Program

- An agency wide information security program includes:
- security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of
- information security risks associated with their activities; and
- their responsibilities in complying with agency policies and procedures designed to reduce these risks.

Reporting Requirements

- Each agency shall (1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter…

Annual Independent Evaluation

- Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

Annual Independent Evaluation (continued)

- for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the Agency, and
- for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

Training Questions in Last Year's GISRA Report

- For FY01 and FY02, number and percentage of agency employees including contractors that received security training. FY01 _#_ and _%_, FY02 _#_ and _%_
- For FY01 and FY02, number of employees with significant security responsibilities. FY01___ and FY02___.
- For FY01 and FY02, number of employees with significant security responsibilities that received specialized training. FY01 _#_ and _%_, FY02 _#_ and _%_.
- Briefly describe what types of security training were available during the reporting period, and for FY01 and FY 02, the total costs of providing such training. FY01___ and FY02___.

Employee Training
Cross Cut of Small and Independent Agencies

- 57 agencies reporting
- Nine reported annual security training for 100% of their staff.
- Twelve reported that they trained less than 10% of their staff.
- Six agencies did not record the number of employees trained.
- Remainder reported training a moderate number of their workforce.

Types of Employee Training Reported

- Orientation
- Annual refresher training
- Specialized training (i.e. for users of laptops)

Methods of Employee Training

- Self study CDs
- Videos
- Websites with automated tracking systems
- Personal instruction

Training for Employees with Significant Security Responsibilities

- Of 1032 employees with significant security responsibilities at the small and independent agencies, 387 (37%) received training in FY02.

Types of Training

- Firewall maintenance
- Auditing
- Contingency planning

Methods of Training

- Government seminars
- Vendor training

Where do we go from here?

- OMB will issue implementing guidance for FISMA.
- Information will continue to be collected about agency security training programs