OIG INFORMATION TECHNOLOGY SECURITY AUDITS AND *THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) OF 2002*

Andy Patchan, Assistant Inspector General for Audits and Attestations
Office of Inspector General
Board of Governors of the Federal Reserve System
Federal Information Systems Security Educators Assocation Conference
March 25, 2009

Background

- FISMA was enacted in 2002 in response to increasing reports of computer intrusions and IT security weaknesses
- Requires the Head of each federal agency to:
  - Provide information security commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of the information and systems

Background (cont.)

- Requires the Chief Information Officer of each agency to designate a Senior Agency Information Security Officer to carry out the Act's security responsibilities
- Assigns the National Institute of Standards and Technology the responsibility to develop appropriate IT security standards
- Requires each agency to develop, document, and implement an agencywide information security program

Requirements of an Agencywide Information Security Program

- Risk assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or systems
- Policies and Procedures, based on the risk assessments, that cost-effectively reduce information security risks to an acceptable level, through the lifecycle of each system

Requirements of an Agencywide Information Security Program (cont.)

- Periodic Testing and Evaluation of the effectiveness of information security policies, procedures, and practices, performed at least annually but more frequently depending on risk
  - Must include testing of management, operational, and technical controls of every system in the agency's systems inventory
- A process for planning, implementing, evaluating, and documenting corrective actions to address any deficiencies

Requirements of an Agencywide Information Security Program (cont.)

- Procedures for detecting, reporting, and responding to security incidents, including
  - Mitigating risks with such incidents before substantial damage is done, and
  - Notifying and consulting with law enforcement agencies and relevant Offices of Inspector General

Requirements of an Agencywide Information Security Program (cont.)

- Security awareness training to inform personnel and contractors of:
  - Information security risks associated with their activities
  - Their responsibilities in complying with agency policies and procedures to reduce these risks
- Plans and procedures to ensure continuity of operations of information systems

Office of Inspector General (OIG) Statutory Responsibilities

- To conduct and supervise audits and investigations relating to the agency's programs and operations;
- To promote economy, efficiency, and effectiveness, and
- To prevent and detect fraud and abuse in programs and operations.

Requirements for OIG FISMA Evaluations

- Perform an annual independent evaluation of the effectiveness of the agency's information security program and practices
  - Test of a representative subset of systems
  - Assess the agency's compliance with information security policies, procedures, standards, and guidelines.
  - Report the evaluation results by end of September to the Agency and the Office of Management and Budget
  - Office of Management and Budget reports on summary of all agencies progress and OIG evaluations by March 1 of each year.

Accomplishments from Agency and OIG FISMA Evaluations

- Office of Management and Budget reported in its FY 2007 FISMA report to Congress, that in the 6 years since the 2002 Act:
  - The number of systems certified and accredited has risen from 47% to 92%
  - The number of systems with tested security controls has risen from 60% to 95%
  - The number of systems with tested contingency plans has risen from 35% to 86%
- But additional and continued management attention needed on risk assessments and security testing

Congressional Interest in Strengthening FISMA

- Revised GAO FISCAM
- FISMA Improvement Bill
- GAO Review of Best Practices on IT Security Metrics

- QUESTIONS??