FISMA Lessons Learned

Beth Serepca

Team Leader OIG

U.S. Nuclear Regulatory Commission

March 13, 2008

House Hearing on Federal IT Security: "The Future of FISMA," June 7, 2007

"When it comes to information security, the federal government can and *should be the leader.* FISMA requires each agency to create a *comprehensive risk-based approach* to agency-wide information security management. It is intended to make security management an *integral part* of an agency's operations and to ensure we are actively using *best practices* to secure our systems.

Sure, the law has its critics – mainly from failing agencies and those who misunderstand what it was designed to do. Certainly, we want to avoid a "check the box" mentality. We need to incentivize strong information protection policies. *We need to pursue a goal of security rather than compliance.* "

Opening Statements
Ranking Minority Member, Tom Davis

Benefits and Challenges with Annual FISMA Reporting

- Improving collaboration between the Office of Inspector General (OIG) and Chief Information Officer (CIO)
- Providing fast-paced reporting that addresses changing IT security threats and requirements
- Increasing awareness of IT security risks and need for senior management attention
- Paving new ground in the absence of a standard methodology for assessing information security programs and system controls
- Considering both internal and external security controls and impact on agency operations

Improving Collaboration between the OIG and the CIO to Achieve FISMA Objectives

- Working together, CIOs and IGs are improving the quality of agencies' C&A and POA&M processes
- Audits promote a risk-based approach by considering progress toward agency-specific IT security goals
- Audit standards ensure quality results and help to resolve potential disagreements
- Verifying technical controls through collaborative test procedures confirms status of required system security controls
- New operational procedures promote fast-paced reporting and better address the changing e-gov environment

Paving New Ground with Information Security Program and System Security Audits

- Developing and implementing IT audit skills, tools, and test procedures in support of FISMA
  - Building audit teams with specialized skills in information security
  - Vulnerability, database, and web application scanning tools
  - Audit methodologies that cover NIST SP 800-53 control families and address high risk issues
- Assessing controls for sensitive data including personally identifiable information, financial, and mission-specific information
- Privacy control audits overlapping with FISMA

Increasing Awareness of IT Security Risks and Need for Senior Management Attention

- OMB's summary report on GISRA, FY 2001 identified six common weaknesses:
  - 1. Senior management attention
  - 2. Security education & awareness
  - 3. Measuring performance
  - 4. Funding and integrating security into capital planning and investment control (making IT security part of the business process)
  - 5. Ensuring contractor services are adequately secure
  - 6. Detecting, reporting, and sharing information on vulnerabilities

Increasing Awareness of IT Security Risks and Need for Senior Management Attention (continued)

- GAO-08-496T Information Security: "Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies"

  Despite reported progress, federal agencies continue to confront long standing information security control deficiencies.

Common Concerns Regarding Information Security

- Federal Agency Data Protection Act bill
- OMB does not support legislation as stated.

Lessons Learned with FISMA Audits

- Successful IS program implementation requires shared goals, clear roles and responsibilities, and agencywide and system-level performance measures
- Working closely with both system owners, the CIO, and system security officials to identify risks and vulnerabilities and verify security controls
- Changing threat, vulnerability, and control environment calls for continual infusion of new audit methodologies, skills, tools, and training
- Considering both internal and external security controls
- Communication and collaboration with other teams including system, program, and financial statement auditors and other stakeholders

Questions & Contact Info.

Beth Serepca

Team Leader, OIG

Nuclear Regulatory Commission

Beth.Serepca@NRC.GOV

301-415-5911