Office of Inspector General Reviews Under the Federal Information Security Management Act (FISMA)

Presentation to the
Information Security and Privacy Advisory Board
March 4, 2011

Andy Patchan
Associate Inspector General for Audits and Attestations
Federal Reserve Board of Governors

Table of contents

OIG Responsibilities Under FISMA

- OIGs are required by FISMA to perform an annual evaluation to determine the effectiveness of the agency's information security program and practices:
  - An assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines.
  - Testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency's information systems.

FISMA Provides a Structured Process for Assurance of Information Security

- Risk assessments of the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or systems.

- Policies, procedures, and security plans that determine controls needed to cost-effectively reduce risks to an acceptable level.

FISMA Provides a Structured Process for Assurance of Information Security (Cont.)

- Periodic testing and evaluation of the effectiveness of policies, procedures and controls.
- Process for planning, implementing, evaluating, and documenting corrective actions to address deficiencies.
- Security awareness training.
- Plans and procedures for ensuring continuity of operations of information systems.
- Procedures for detecting, reporting, and responding to security incidents.

OIG FISMA Reviews Combine Information Security Structured Processes with Control Effectiveness Metrics

- FISMA has accomplished the institution of information security basic building blocks which provide a foundation for information security.

- OIG reviews have analyzed agencies' information security processes and controls under FISMA:
  - Compare processes and controls against NIST standards.
  - Analyze risk assessments and controls implemented given the vulnerabilities identified.
  - Identify root causes of deficiencies that need to be corrected - - improvements that are needed in the underlying foundation processes to provide assurance that program goals are accomplished.

OIG FISMA Reviews Have Identified that Agencies Made Progress in Information Security under FISMA

- Since FISMA was enacted in 2002 through 2009, OMB has reported federal agencies have achieved measurable information security improvements:

Percentage of Systems with a:	**FY 2002**	**FY 2003**	**FY 2004**	**FY 2005**	**FY 2006**	**FY 2007**	**FY 2008**	**FY 2009**
Certification and Accreditation	47%	62%	77%	85%	88%	92%	96%	95%
Tested Contingency Plan	35%	48%	57%	61%	77%	86%	92%	86%
Tested Security Controls	60%	64%	76%	72%	88%	95%	93%	90%
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	10,304	10,679	12,930

OIG FISMA Reviews From 2005 Through 2008

- Starting in 2005 and going through 2008, OMB FISMA reporting guidance included questions on quality of information security control processes, such as Certification and Accreditation (C&A), but without clear definitions of quality categories:
  - **FY 2005 Government-wide Summary – OIG Answers on Quality of agency C&A process**
    Excellent: 1; Good: 4; Satisfactory: 12; Poor: 8; Failing: 0
  - **FY 2006 Government-wide Summary -- OIG Answers on Quality of agency C&A process**
    Excellent: 2; Good: 6; Satisfactory: 8; Poor: 8; Failing: 1
  - **FY 2007 Government-wide Summary – OIG Answers on Quality of agency C&A process**
    Satisfactory or better: 76%
  - **FY 2008 Government-wide Summary -- OIG Answers on Quality of agency C&A process**
    Excellent: 2; Good: 6; Satisfactory: 15; Poor: 1; Failing: 1

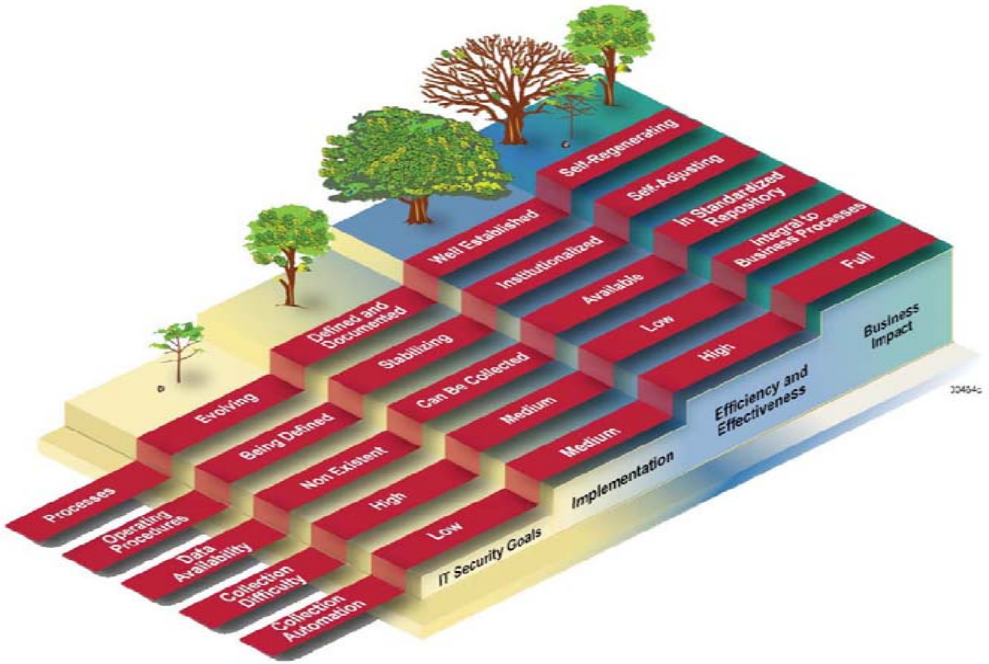
OIGs Recognized the Need to Measure the Maturity of Agency Information Security Programs, Policies, and Procedures

- FISMA requires agencies to follow NIST guidance in implementing their security programs, such as NIST SP 800-53 "Recommended Security Controls for Federal Information Systems and Organizations," and NIST SP 800-55 "Performance Measurement Guide for Information Security."

- NIST 800-55 discusses the different maturity levels for information security, and how opportunities for measurement vary depending on the information security program maturity.

Measuring the Maturity of Agency Information Security Programs, Policies, and Procedures

- NIST maturity model:



OMB's 2009 FISMA Guidance Included OIG Input for Improved Qualitative Reviews

- In 2009, OIG reviews were intended to independently assess if the agency is applying a risk-based approach to their information security programs and the information systems that support the conduct of agency missions and business functions.

- For example, when reviewing the Certification and Accreditation (C&A) of an individual system, the OIG would generally assess whether: 1) the C&A was performed in the manner prescribed in NIST guidance and agency policy; 2) controls were being implemented as stated in any planning documentation; and 3) continuous monitoring was adequate given the system impact level of the system and information.

- Overall, 90% of the agencies had certification and accreditation policies in place that were generally compliant with requirements and guidance.

Building Upon 2009 OIG FISMA Reviews, the 2010 OIG FISMA Reviews Assessed Program Maturity

- The OIG community commented to OMB that they thought it would be helpful to have an assessment of the information security program maturity, and metrics at that maturity level with a focus on continuous monitoring.
- Information security metrics need to be meaningful and provide quantitative measurement. Past FISMA guidance for OIGs has been subjective and lacked criteria for assessment
- Metrics do not have to include only numbers; metrics could include an assessment of the maturity level, such as are there written policies in place, have the policies been fully implemented, is testing adequate to ensure controls are sufficient and operating effectively, and are corrective actions in place to remedy deficiencies and root causes.
- The metrics need to provide for independent, objective review of the status of information security efforts for reporting to top management and agency senior leadership.
- Information security metrics need to be understandable to top management who lack information security expertise.
- Top management visibility into and monitoring of information security is critical for assuring information security progress and assigning the resources needed.

2010 OIG FISMA Review Approach

- In January 2010, the Federal Audit Executive Council (FAEC) IT committee, under the Council of IGs for Integrity and Efficiency, developed draft OIG FISMA reporting metrics created by committee members representing 20 OIGs.
- The overall approach was discussed with OMB, GAO, DHS, and the Federal CIO, all who provided positive feedback.
- The metrics were then provided to all Assistant Inspectors General for Audit members of the FAEC. Suggestions and comments were incorporated, including developing criteria for OIGs to use in evaluating agencies' information security programs.
- In February 2010 we provided our suggestions to OMB.

2010 OIG FISMA Review Approach (cont.)

- OMB provided the following ten categories for the OIGs to focus their analysis on:
  - Certification and Accreditation
  - Configuration Management
  - Security Incident Management
  - Security Training
  - Remediation/Plans of Actions and Milestones
  - Remote Access
  - Identity Management
  - Continuous Monitoring
  - Contractor Oversight
  - Contingency Planning

2010 OIG FISMA Review Approach (cont.)

- The approach required the OIGs to determine for each category whether the agency has:
  - (a) Established and is maintaining a program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes certain attributes.
  - (b) Established and is maintaining a program. However, the Agency needs to make significant improvements as noted.
  - (c) Not established a program.

Example of the 2010 OIG FISMA Review Approach

- Certification and Accreditation

- The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

  - Documented policies and procedures
  - Establishment of accreditation boundaries
  - Categorizes information systems
  - Applies applicable minimum baseline security controls
  - Assesses risks and tailors a security control baseline
  - Assessment of the management, operational, and technical security controls
  - Risks to Agency operations, assets, or individuals are analyzed and documented in the system security plan, risk assessment, or an equivalent document
  - The accreditation official is provided (i) the security assessment report; (ii) the plan of action and milestones; and (iii) the updated system security plan.

Criteria used to Develop 2010 OIG FISMA Review Approach

- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (SP) were used as criteria under the 2010 OIG FISMA review approach

- The following was used as criteria for Certification and Accreditation:

  - FIPS 199-Standard for Categorization of Federal Information and Information Systems
  - FIPS 200-Minimum Security Requirements for Federal Information and Information Systems
  - SP 800-18-Guide for Developing Security Plans for Federal Information Systems
  - SP 800-30-Risk Management Guide for Information Technology Systems
  - SP 800-37-Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life-Cycle Approach
  - SP 800-53-Recommended Security Controls for Federal Information Systems and Organizations
  - SP 800-53A-Guide for Assessing the Security Controls in Federal Information Systems and Organizations
  - SP 800-60-Guide for Mapping Types of Information and Information Systems to Security Categories

2010 OIG FISMA Results for CFO Agencies

Cyber Security Program Area	Compliant Program		Needs Improvement		Program Not Implemented	
	No.	%	No.	%	No.	%
Security Authorization	13	54	11	46	0	0
Configuration Management	6	25	18	75	0	0
Incident Response	15	62	9	38	0	0
Security Training	7	29	17	71	0	0
POA&M	8	33	16	67	0	0
Remote Access	10	42	14	58	0	0
Account and Identity Management	5	21	19	79	0	0
Continuous Monitoring	7	29	15	63	2	8
Contingency Planning	8	33	16	67	0	0
Contractor Oversight	6	25	16	67	2	8

Questions

?