OIG FISMA Reporting: 2014 FISMA Modernization Act and IG Maturity Model for Information Security Continuous Monitoring (ISCM)

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD
IG Panel

June 10, 2015

Council of the Inspectors General on Integrity and Efficiency

Discussion Points

- FISMA Modernization Act
- Proposed maturity model for OIGs' 2015 FISMA reviews of agencies' ISCM programs
- References for proposed ISCM maturity model
- Progress to date

Requirement for Annual OIG FISMA Reviews

- Both 2002 FISMA (2002 E-Gov Act) and December 2014 FISMA Modernization Act requirement for annual OIG reviews:
  - 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.

FISMA Modernization Act Changes Pertaining to OIG FISMA Reviews

Each evaluation under this section shall include

2002 FISMA		FISMA Modernization Act
• **"(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;**	=	• **"(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;**
• **(B) an assessment (made on the basis of the results of the testing) of compliance with** • **(i) the requirements of this subchapter; and** **(ii) related information security policies, procedures, standards, and guidelines."**	≠	• **(B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency."**

NIST 800-53 Definition of Effectiveness

"Security control effectiveness addresses the extent to which the controls are **implemented correctly, operating as intended, and producing the desired outcome** with respect to meeting the security requirements for the information system in its operational environment."

Other Changes in the FISMA Modernization Act Relating to OIG FISMA Reviews

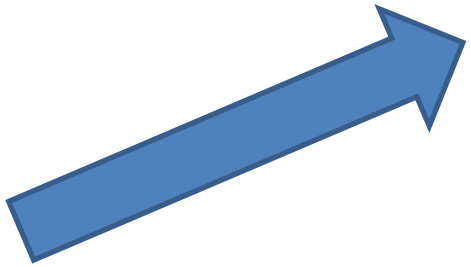
- **Assessment technical assistance**
  - The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as applicable, to assist the Inspector General or head of an agency in carrying out their duties under this section including by testing information security controls and procedures.

- **Guidance**
  - The Director, in consultation with the Secretary, the CIO Council, the CIGIE, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices.

Proposed IG ISCM Maturity Model

ISCM Attributes

1.1.1 Documented policies and procedures for ISCM
1.1.2 Documented strategy for ISCM that includes consideration of risk assessments
1.1.3 Implementation of ISCM for IT assets and performance of security controls assessment
1.1.4 ISCM reporting



Level 1 Ad-hoc

ISCM policies, procedures, and strategy not formalized; ISCM activities performed in an ad-hoc, reactive manner

Level 2 Defined

ISCM policies, procedures, and strategy are formalized and documented but not consistently implemented

Level 3 Consistently Implemented

ISCM policies, procedures, and strategy are consistently implemented and agency performs validation testing. However, quantitative and qualitative effectiveness measures are lacking

Level 4 Managed & Measurable

Quantitative and qualitative measures on the effectiveness of ISCM policies and procedures are collected across the organization and used to assess the ISCM program and make necessary changes

Level 5 Optimized

ISCM policies, procedures, and strategy are fully institutionalized, repeatable, self generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Example Dashboard for OIG ISCM Maturity Model

ISCM Attribute	Ad-hoc	Defined	Consistently Implemented	Managed & Measurable	Optimized	Attribute Maturity Level
ISCM policies & procedures						3
ISCM strategy and risk assessment						3
Implementation for IT assets & security controls assessment						2
Security status reporting						2

ISCM Program Overall Maturity Level: 2

References Used

- NIST Cybersecurity Framework
- NIST Special Publications
- Electricity subsector cybersecurity capability maturity model
- CoBIT maturity model
- ISO maturity model

Progress to Date

- Briefed Inspectors General in May 2014
- Met with OMB, DHS, GAO, NIST, and Federal CIO Council in summer/fall 2014
  - Received positive feedback and overall support
- Discussed maturity model approach with members of the FAEC IT Committee (under the CIGIE Audit Committee), which includes representatives from 38 OIGs
  - Formed maturity model workgroup consisting of representatives from 9 OIGs – Treasury, FDIC, HUD, VA, Transportation, TIGTA, Interior, CNCS, and FRB/CFPB – have been meeting on monthly basis since Fall 2014
- Regular briefings to CIGIE IT Committee on progress
- Met with OMB, DHS, GAO, and NIST, to obtain comments – March/April 2015
- DHS to incorporate maturity model into FY 2015 OIG FISMA metrics – June 2015
- Work on maturity model for other information security areas for FY 2016 FISMA reviews