

OIG Panel on FISMA

1

**PRESENTED TO THE
INFORMATION SECURITY AND PRIVACY
ADVISORY BOARD**

FEBRUARY 13, 2012

Key Questions Posed....



- What is covered in a FISMA audit?
- Does closing of audit findings = increased security?
- Is it appropriate that agency IG FISMA reports are given as much weight as the agency submissions themselves?
- Are there additional ways to leverage the role of the IGs to ensure FISMA compliance?
- How to quantify return on audit resources – how are the results used in multiple assessments and decisions?
- When we get to cloud, how should we think about auditing & forensics as part of the service contract?
- How are evaluations conducted on systems managed or owned by third parties?

FISMA Framework



OMB
DHS

Cyberscope

Privacy FISMA
Report
(Sept 30)

Cyberscope
10 questions
PII in nature

CIO
FISMA Report
(Sept 30)

Plan of
Actions and
Milestones
(POA&M)

Cyberscope
31 questions

POAM findings from
NSF Continuous Monitoring
OIG IT audit
FISMA
Fin Stmt (IT)

OIG
FISMA
Report
(Sept 30)

OIG FISMA
Narrative
Report
(optional)

Cyberscope (11 ?s)
C&A CM
CIRT Training
POAM Remote Access
Access Cntls Cont Monitoring
DRP Contractor Systems

Narrative Report
IT Findings tracked A-50

Audited
Financial
Statement
Report
(Sept 30)

Financial reporting
CFO Act
FISCAM
SP 800-53
IT findings tracked A-50

IT work conducted per
FISMA
FISCAM
CFO Act
SP 800-53 (Controls)
SP 800-37 (C&A)

OIG Responsibilities Under FISMA

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

2012 FISMA Reporting Metrics for IGs

- DHS FISMA guidance directs the OIGs to focus their reviews on:
 - ✦ Risk management
 - ✦ Continuous monitoring
 - ✦ Incident response and reporting
 - ✦ Security training
 - ✦ Plan of actions and milestones
 - ✦ Remote access management
 - ✦ Identity and access management
 - ✦ Configuration management
 - ✦ Contingency planning
 - ✦ Contractor systems
 - ✦ Security capital planning

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

NIST Maturity Model

