OIG Responsibilities under FISMA

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

IG Panel

June 10, 2015

Brett M. Baker, PhD, CPA, CISA
Assistant Inspector General for Audit
National Science Foundation

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

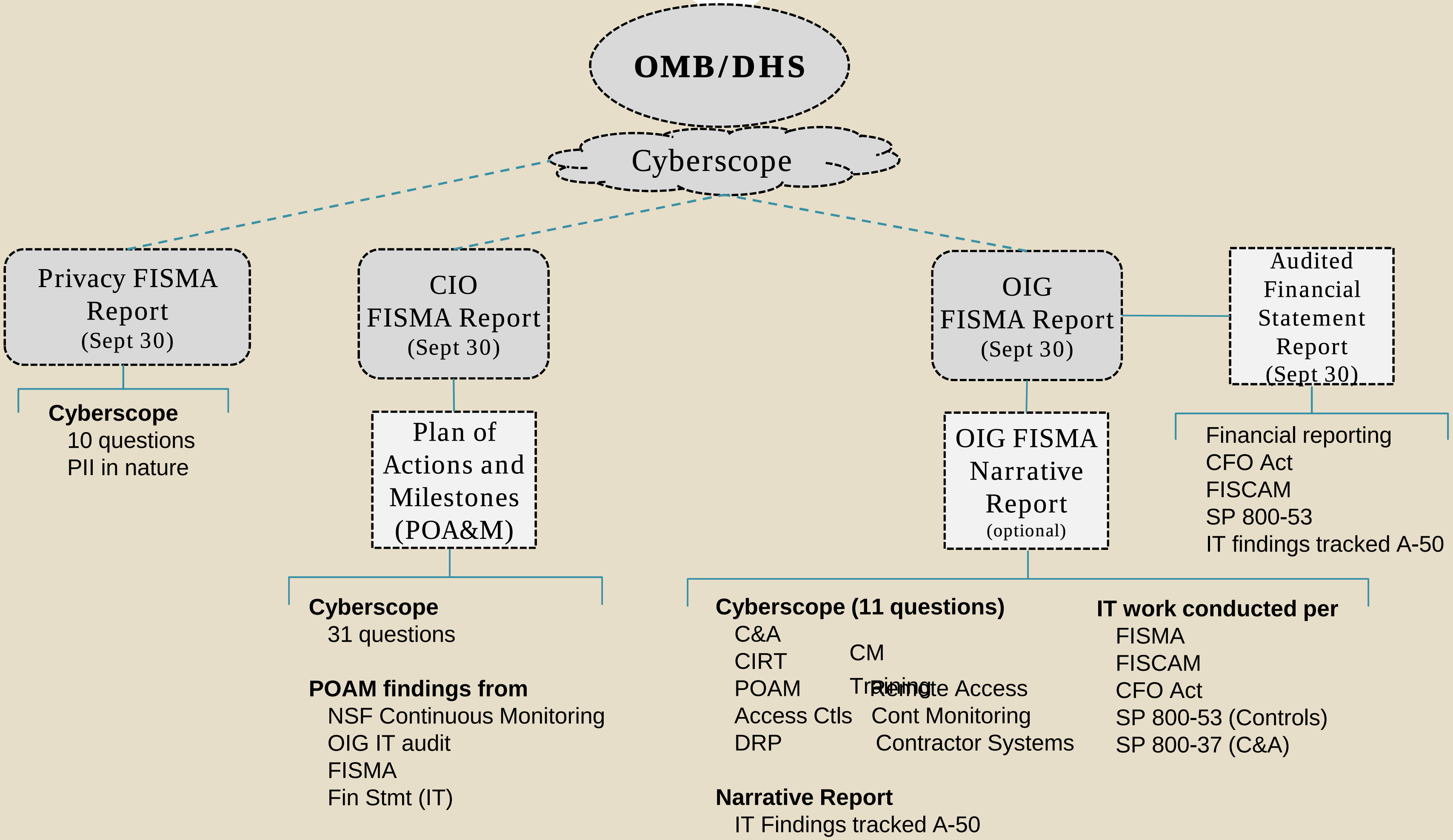
    - Testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency’s information systems

    - An assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines

OIG focus areas under FISMA

- DHS FISMA guidance directs 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

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 questions)
C&A
CIRT
POAM
Access Ctls
DRP
CM
Training
Remote Access
Cont Monitoring
Contractor Systems

Narrative Report
IT Findings tracked A-50

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

Audited Financial Statement Report (Sept 30)

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

FISMA Updates 2014-2015

2014 Updates

- Agencies are required to submit an information security strategy to Cyberscope by November 2014.

2015 Updates

- Cyberscope reporting will include outcome-oriented measures to better assess the status of agencies' information security posture.
- DHS initiative for formalized process for regular and proactive scans of public agency networks. DHS first needs to obtain authorization from the agency.
- Updates DHS US-CERT Incident Notification Guidelines for reporting information security incidents to DHA US-CERT. Format will allow for more consistency.
- OIGs will assess the effectiveness of agency continuous monitoring programs using a capability maturity model.

Questions?

Dr. Brett M. Baker

NSF Assistant Inspector General for Audit

703-292-7100

oig@nsf.gov