Federal Information Security Management Act: A Perspective

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

OIG Panel

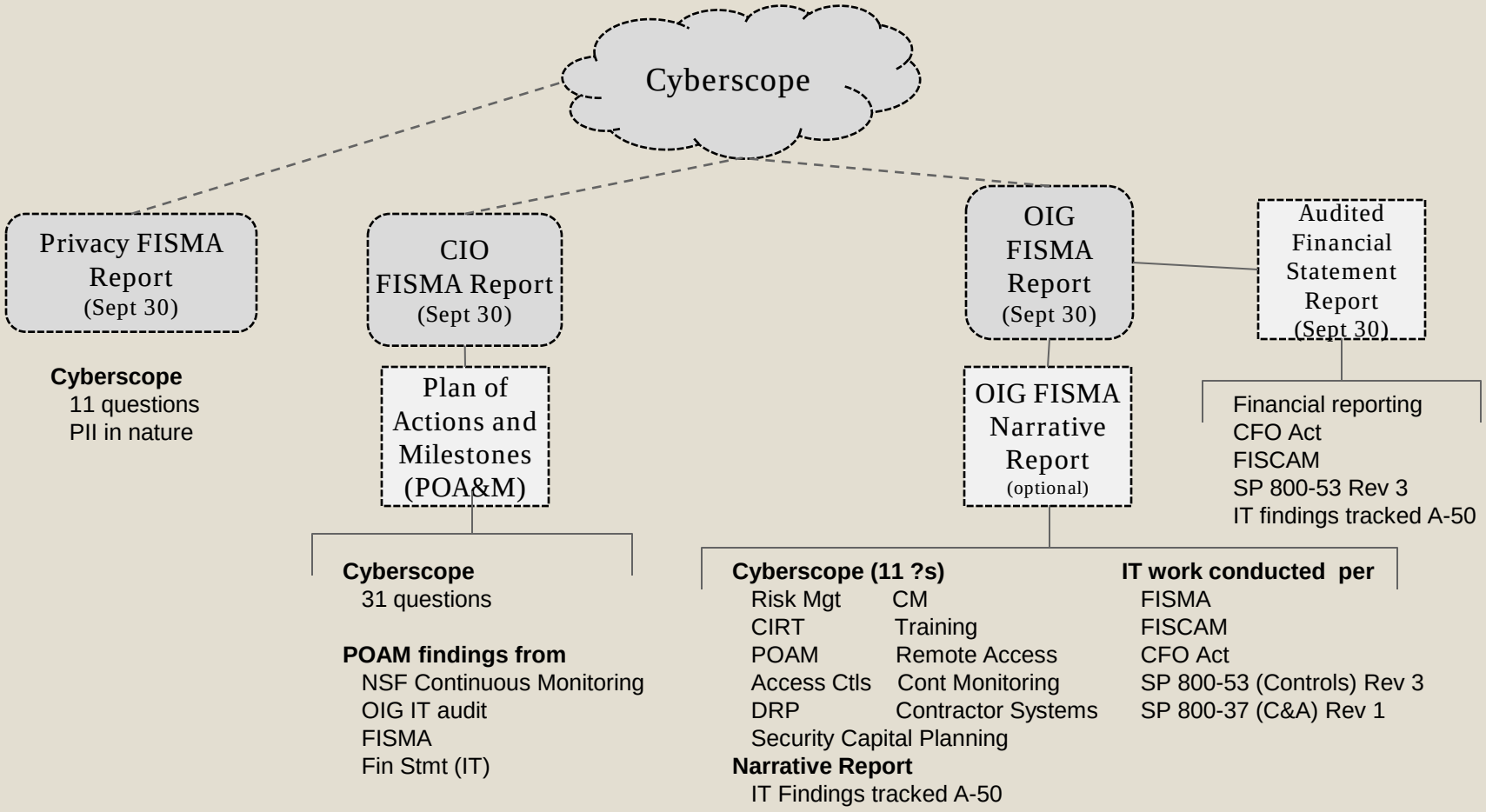
October 10, 2012

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

FISMA Overview at NSF

- $ 6.2B in Research and Education Grants in 2011
- Over 61,000 requests for funding via electronic submission – intellectual property (2012)
- FISMA review is contracted to CPA firm
- 2011 FISMA OIG Cyberscope and Narrative Report
- FISMA coverage: 8 agency systems (3 contractor)

FISMA Framework



FISMA Overall Effect

- Improved security posture across government
  - Continued focus on information security by senior officials
  - Improvements from audit recommendations

FISMA Report Issues

- Network architecture is not addressed in the questions
- Point in time status, not continuous monitoring
  - Response to issues during year is not reported
- Some Y / N questions instead of narrative answers

FISMA 2012

- Automated and continuous monitoring
- Reporting of security incidents
- Compliance with NIST Standards
- Director of OMB - oversight authority
- No additional funding

Suggestions

- Supplement OMB questionnaire with a narrative report
- Ensure FISMA and Financial Statement auditors communicate results to each other

Questions?

Dr. Brett M. Baker

NSF Assistant Inspector General for Audit

703-292-7100

oig@nsf.gov