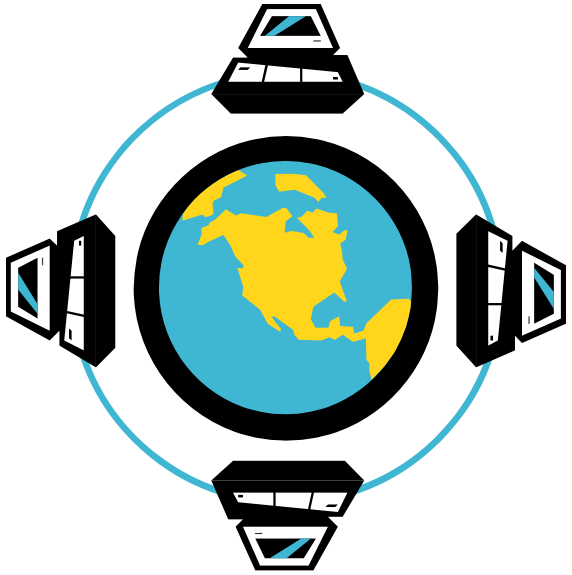
FISMA and the IGs

ISPAB

IG Panel

March 4, 2011



Presenter:

Louis C. King

Program Director, DOT/OIG

Agenda

- IG Community Contributions
- FISMA Purpose
- Recommended Changes to FISMA
- Comments to Proposed Legislative Changes
- Audit vs. Evaluation
- Q&A
- Presenter Bio

IG Community Contributions

- Worked with OMB and DHS to redefine metrics to be used for 2010
- Provided input into OMB government wide FISMA report
- Established CIGIE Cyber Security Working Group

Recommended Changes To FISMA

- Clarifying authority of CIO and CISO to ensure responsibilities align with authority
- Establish statutory deadlines for FISMA results
- Mandate assessment of agencies' information security maturity level based on NIST model

Recommended Changes To FISMA

- Require reviews of personnel performing information security work
- Define inherently governmental roles and required security clearances needed in the cyber security process

Comments to Proposed Legislative Changes

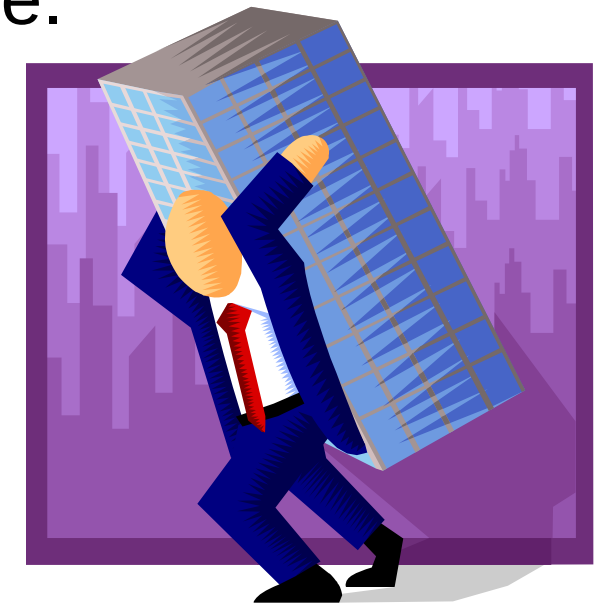
- OIG involvement in conducting reviews is essential and should remain in legislation.
- OIGs should continue to conduct annual reviews. The benefits of annual reviews outweighs the risks of conducting less frequent reviews.
- OIGs audit independence must remain intact to successfully perform OIG audits.

Audit Vs. Evaluation

- DOT OIG supports conducting FISMA audits as opposed to evaluations.
- The benefits of conducting an information security audit outweighs the cost.
  - Improves timeliness of findings thereby enabling more timely resolution of weaknesses
  - Better basis to reach conclusions
  - More comprehensive results
  - Greater awareness of FISMA/Cyber Security

Audit Vs. Evaluation

- For 2011, DOT OIG plans to review 71 of 400+ DOT systems. This will allow stratifying by sub-components while obtaining an adequate level of audit assurance.



Audit Vs. Evaluation

- Potential issues of mandating audits
  - Requires IGs to make a conscious decision to refocus limited resources to FISMA
  - Diminishes the ability for IGs to conduct other audits

Questions?

Presenter Bio & Contact Info

- Louis C, King is the Program Director at DOT OIG responsible for conducting FISMA audits. He is a CPA, CISA, CGFM, CMA and CFM. He has directed 8 FISMA audits (5 for Treasury and 3 for DOT) and numerous other IT related audits. Prior to directing IT audits, he was a Director of Financial Audits.
- 202-366-4350
- Louis.King@oig.dot.gov