SSA OIG's Use of Contractors to Comply with FISMA

Presented by
Gale Stone
Office of the Inspector General
Deputy Assistant Inspector General for Audit
Social Security Administration

SSA's Information System Infrastructure

- Oversees $1,668 billion of assets and pays out $536 billion in benefits (annual estimates) to over 52 million beneficiaries.
- Processes over 252 million earning records annually and maintains a database of over 400 million earnings records.
- Consists of 20 major systems that process information from over 1,500 field offices, regional offices, teleservice centers, program services centers and hearing offices. Each system is certified and accredited.
- Most major systems tied directly into the production of the Financial Statements.

OIG's efforts to comply with CFO requirements

- SSA hired PwC as our independent auditor in 1997 to review SSA's financial statements.
- PwC performs a wide range of internal control testing including:
  - Security tests based GAO's Federal Information System Control Audit Manual.
  - Additional security testing including internal and external penetration testing when needed.

FISMA Requirements

- Agencies are required to develop and maintain an agency-wide information security program.
- Agencies perform an annual evaluation of information security program.
- OIG's perform an annual independent evaluation of Agencies' security program.

SSA OIG Approach to FISMA

- Since PwC's F/S audit includes extensive testing of IS controls, OIG contracted with PwC to perform additional steps to evaluate Agency's compliance with FISMA.
- SSA did not want an opinion of its IS security program.
- OIG decided that the additional contract vehicle with PwC would be an Agreed-Upon-Procedures (AUP) engagement.

FISMA AUP Engagement

OIG contracted with PwC to perform an AUP engagement using the following criteria:

1. FISMA
2. OMB Memorandum M-06-20
3. NIST Guidance
4. Other relevant security laws and regulations

SSA's Approach to FISMA

- Each major system owner completed the NIST Self-Assessment Guide (questionnaire).
- The Agency engaged Deloitte & Touche (D & T) to conduct an independent assessment on the Agency's IT security program using FISMA and NIST questionnaire for IT systems.
- Agency drafted its own report in accordance with the OMB guidance.
- Agency emphasized "Getting to Green" for the security portion of President's eGov initiative.

SSA/OIG/PwC Communication

- Coordinated review efforts/steps.
- FISMA status meetings held with the Agency to discuss
  1. Issues (findings)
  2. Current status
  3. What is required to resolve issue
- Exchanged draft FISMA reports with the Agency prior to issuance of final FISMA reports.
- OIG review follow-up actions.

FISMA Accomplishments

- SSA and the OIG have met the FISMA reporting requirements every year.
- Agency took action on OIG's recommendations:
  - Agency improved its POA&M process
  - Agency developed a systems inventory
  - Agency added staff to CIO's office

Plans for next year

- Continue with current approach.
- Follow-up with the Agency on prior year findings.
- Modify according to OMB guidance update.

FISMA Lessons Learned

Contractor should:

- work closely with the Agency.
- clearly define plan/strategy.
- begin work as early as possible.
- Where possible, rely on prior work.

QUESTIONS!