GAO Information Security Update

Presented to

Federal Computer Security Program Managers’ Forum

June 12, 2012
Agenda

- Snapshots of Federal Information Security
- Ongoing and Planned Work
- Current Bills to Amend FISMA
- Recent GAO Reports
- Questions
• Agencies have provided training to increasing percentages of personnel
Snapshots of Federal Information Security (cont.)

• Agencies have increased automated capabilities for managing assets
Snapshots of Federal Information Security (cont.)

- Most agencies had weaknesses in most FISCAM general control areas in FY 2011
Snapshots of Federal Information Security (cont.)

- Agencies continue to report information security weaknesses over financial systems

Source: GAO analysis of agency performance and accountability reports, annual financial reports, or other financial statement reports for fiscal year 2011.
Snapshots of Federal Information Security (cont.)

- Reported security incidents continue to rise

Snapshots of Federal Information Security (cont.)

• Agencies reported a variety of incidents

[Diagram showing the distribution of incidents with the following breakdown:]
- Investigation: 0%
- Denial of service: 7%
- Scans/probes/attempted access: 16%
- Unauthorized access: 19%
- Improper usage: 27%
- Malicious code: 31%

Snapshots of Federal Information Security (cont.)

• Common recommendations for improving security controls:
  • Change vendor-supplied IDs and passwords
  • Strengthen authentication controls
  • Use two-factor authentication for remote access
  • Limit access to bona fide needs
  • Remove inactive accounts & accounts of separated users
  • Install patches timely
  • Keep software current
  • Use encrypted protocols
  • Implement access control lists
Snapshots of Federal Information Security (cont.)

- Common recommendations for improving security programs:
  - Provide role-based training for those with significant security responsibilities
  - Monitor assets, configurations, vulnerabilities frequently
  - Test effectiveness of IT security controls
  - Remedy known vulnerabilities timely
  - Verify effectiveness of remediation efforts
  - Implement adequate incident detection and response capabilities
  - Test viability of contingency plans
Snapshots of Federal Information Security (cont.)

• Current federal priorities for enhancing cybersecurity
  
  • TIC/Einstein
    • External connections
  
  • Continuous monitoring
    • Automated monitoring capabilities
    • Cyberscope
  
  • HSPD-12, PIV Cards
    • Logical access
Ongoing and Planned Work

FISMA
- Mandate Report and Analysis
- EPA
- Census Bureau
- FCC

Emerging Issues
- Implantable Medical Devices
- Security of Mobile Devices
- Cybersecurity Strategies

Privacy
- Electronic Prescriptions
- Wireless Location-Based Information

Consolidated Financial Statements
- IRS
- BPD/Federal Reserve
- FDIC
- SEC
- OIGs
- TARP
- FHFA
- SOSI
- CFPB

Critical IT Systems & Infrastructure
- Fed. Role in Datacomm Network Security
- Cyber Threats to DOD Industrial Base

Training/Methodology/Liaison
- FISCAM
- GAO Internal Controls
- Internal/External Training
- Technical Assistance to Hill
- OMB/NIST/NASCIO
Current Bills to Amend FISMA

• **Four bills introduced to amend FISMA**
  - Lieberman/Collins(S 2105), McCain/Hutchinson(S 2151), Issa/Cummings(House passed HR 4257), and Langevin/Bartlett (HR1136)

• **Major Issues**
  - Disparity in oversight of agency information security programs (OMB, DHS, Commerce, or National Office for Cyberspace)
  - Emphasis on continuous monitoring, operational capabilities, and incident detection and response
  - Varying approaches on IG evaluations
Recent GAO Reports

- GAO-12-666T, Cybersecurity: Threats Impacting the Nation (April 2012)
- GAO-12-361, IT Supply Chain: National Security-Related Agencies Need to Better Address Risks (March 2012)
- GAO-12-507T, Cybersecurity: Challenges in Securing the Modernized Electricity Grid (February 2012)
Recent GAO Reports

- GAO-12-92, *Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use* (December 2011)
- GAO-12-8, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination* (November 2011)
Recent GAO Reports

- GAO-11-751, *Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards* (September 2011)
- GAO-11-865T, *Cybersecurity: Continued Attention Needed to Protect Our Nation’s Critical Infrastructure* (July 2011)
Recent GAO Reports

- GAO-11-149, *Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain* (July 2011)
Questions
Contacts

**Gregory Wilshusen**  
Director, Information Security Issues  
WilshusenG@gao.gov

**Anjalique Lawrence**  
Assistant Director, Information Security Issues  
LawrenceAJ@gao.gov