GAO Information Security Update

Presented to
Federal Computer Security Program Managers’ Forum

August 20, 2014
Agenda

• Snapshots of Federal Information Security
• Ongoing and Planned Work
• Sense of the Information Security Community
• Recent GAO Reports
• Questions
Agencies largely report increases in security capabilities

<table>
<thead>
<tr>
<th>Capability Area</th>
<th>FY 2012</th>
<th>FY 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Asset Management Information Security Continuous Monitoring (ISCM)</td>
<td>86%</td>
<td>83%</td>
</tr>
<tr>
<td>Automated Configuration Management (ISCM)</td>
<td>70%</td>
<td>79%</td>
</tr>
<tr>
<td>Automated Vulnerability Management (ISCM)</td>
<td>83%</td>
<td>81%</td>
</tr>
<tr>
<td>Trusted Internet Connections Traffic Consolidation</td>
<td>81%</td>
<td>86%</td>
</tr>
<tr>
<td>Personal Identity Verification Logical Access (HSPD-12)</td>
<td>57%</td>
<td>67%</td>
</tr>
<tr>
<td>Portable Device Encryption</td>
<td>90%</td>
<td>84%</td>
</tr>
<tr>
<td>Remote Access Encryption</td>
<td>82%</td>
<td>98%</td>
</tr>
<tr>
<td>Email Encryption</td>
<td>35%</td>
<td>51%</td>
</tr>
<tr>
<td>User Security Training</td>
<td>88%</td>
<td>94%</td>
</tr>
<tr>
<td>Users with Security Responsibility Training</td>
<td>92%</td>
<td>92%</td>
</tr>
</tbody>
</table>

Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013 and OMB’s May 1, 2014 annual report to Congress.
Agencies experienced weaknesses in information security controls

Information security weaknesses

- Access control
- Configuration management
- Segregation of duties
- Continuity of operations
- Security management

Source: GAO analysis of agency, inspectors general, and GAO reports.
Reported security incidents continue to rise

Number of reported incidents

<table>
<thead>
<tr>
<th>Fiscal year</th>
<th>Number of Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>5,503</td>
</tr>
<tr>
<td>2007</td>
<td>11,911</td>
</tr>
<tr>
<td>2008</td>
<td>16,843</td>
</tr>
<tr>
<td>2009</td>
<td>29,999</td>
</tr>
<tr>
<td>2010</td>
<td>41,776</td>
</tr>
<tr>
<td>2011</td>
<td>42,854</td>
</tr>
<tr>
<td>2012</td>
<td>48,562</td>
</tr>
<tr>
<td>2013</td>
<td>61,214</td>
</tr>
</tbody>
</table>

Agencies reported a variety of incidents

Summary of CFO Act Agency Incidents Reported to US-CERT in FY 2013

Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013 and OMB’s May 1, 2014 annual report to Congress.
Ongoing and Planned Work

FISMA
- Mandate Report and Analysis
- VA Information Security
- HHS Components
- High Impact Systems
- Cyber Risk Management

Emerging Issues
- Facility and Access Systems
- DOD Cyber Insider Threat
- DOD Cyber Command
- FedRAMP
- Continuous Monitoring

Privacy
- CFPB Data Collection
- Privacy of facial recognition data
- Privacy of federal and state workforce databases

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

Critical IT Systems & Infrastructure
- Healthcare.gov Security & Privacy
- FAA Air Traffic Control Systems
- Sector Specific Agencies
- NCPS (Einstein)

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

Ongoing and Planned Work
Ongoing and Planned Work – FISMA-related

- Mandated Report
- VA Information Security
- HHS Components
- High Impact Systems
- Cyber Risk Management
Ongoing and Planned Work – Emerging Issues

- Facility and Access Systems
- DOD Cyber Insider Threat
- DOD Cyber Command
- FedRAMP
- Continuous Monitoring
Ongoing and Planned Work – Consolidated Financial Statements

- IRS
- BFS / Federal Reserve
- FDIC
- SEC
- FHFA
- CFPB
- TARP
- SOSI
- OIGs
Ongoing and Planned Work – Critical IT Systems & Infrastructure

- Healthcare.gov Security & Privacy
- FAA Air Traffic Control Systems
- Sector Specific Agencies
- National Cybersecurity Protection System (Einstein)
Ongoing and Planned Work – Privacy-related

- CFPB Data Collection Security & Privacy
- Privacy of Facial Recognition Data
- Privacy of Federal and State Workforce Databases
1. Has your agency’s continuous monitoring processes generated tangible benefits to the assessment and authorization of systems? To the resolution of identified vulnerabilities?
2. If your agency has migrated some of its systems to a cloud environment, does your agency have a clear understanding of how the data is protected in transit or at rest, and where such data resides (e.g. in the U.S. or overseas)?
3. Has your agency’s continuous monitoring efforts been aided, hindered, or unaffected by cloud computing?
Sense of the Information Security Community

4. What are the three biggest challenges you face in securing your agency’s computer networks and systems?
5. How can GAO and OIGs improve their audits and evaluations of information security practices to better assist you in securing your computer networks and systems?
Recent GAO Reports

- GAO-14-344, *Information Security*: Additional Oversight Needed to Improve Programs at Small Agencies (June 2014)
Recent GAO Reports

Recent GAO Reports

Questions
Contacts

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

Larry Crosland
Assistant Director, Information Security Issues
CroslandL@gao.gov