GAO Information Security Update

Presented to
Federal Computer Security Program Managers’ Forum

August 26, 2015
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 2013</th>
<th>FY 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Asset Management Information Security Continuous Monitoring (ISCM)</td>
<td>83%</td>
<td>96%</td>
</tr>
<tr>
<td>Automated Configuration Management (ISCM)</td>
<td>79%</td>
<td>86%</td>
</tr>
<tr>
<td>Automated Vulnerability Management (ISCM)</td>
<td>81%</td>
<td>94%</td>
</tr>
<tr>
<td>Trusted Internet Connections Traffic Consolidation</td>
<td>86%</td>
<td>95%</td>
</tr>
<tr>
<td>Personal Identity Verification Logical Access (HSPD-12)</td>
<td>67%</td>
<td>72%</td>
</tr>
<tr>
<td>Remote Access Authentication</td>
<td>79%</td>
<td>77%</td>
</tr>
<tr>
<td>Portable Device Encryption</td>
<td>84%</td>
<td>55%</td>
</tr>
<tr>
<td>Email Encryption</td>
<td>51%</td>
<td>54%</td>
</tr>
<tr>
<td>User Security Training</td>
<td>94%</td>
<td>93%</td>
</tr>
<tr>
<td>Users with Security Responsibility Training</td>
<td>92%</td>
<td>80%</td>
</tr>
</tbody>
</table>

Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013 and OMB’s May 1, 2015 annual report to Congress.
Agencies experienced weaknesses in information security controls

Federal information system controls audit manual control areas

- Access Control: 22
- Configuration Management: 22
- Segregation of Duties: 15
- Contingency Planning: 18
- Security Management: 23

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

Reported PII incidents are also increasing

Number of reported incidents

<table>
<thead>
<tr>
<th>Fiscal year</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10,481</td>
<td>13,028</td>
<td>15,584</td>
<td>22,156</td>
<td>25,566</td>
<td>27,624</td>
</tr>
</tbody>
</table>

Agencies reported a variety of incidents

- Unauthorized Access: 1,035 (2%)
- Investigation: 1,599 (2%)
- Suspicious Network Activity: 2,198 (3%)
- Social Engineering: 3,967 (6%)
- Malicious Code: 7,413 (11%)
- Equipment: 8,798 (13%)
- Improper Usage: 760 (1%)
- Phishing: 194 (0.3%)
- Denial of Service: 85 (0.1%)
- Non Cyber: 16,879 (25%)
- Scans/Probes/Attempted Access: 12,652 (19%)
- Policy Violation: 11,588 (17%)

Ongoing and Planned Work

FISMA
- Mandate Report
- HHS Components
- High Impact Systems
- Cyber Risk Management
- National Mediation Board

Emerging Issues
- NCPS (Einstein)
- Healthcare.gov Data Hub
- CISO Authorities
- FedRAMP
- Continuous Monitoring
- DHS Cybersecurity Workforce

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

Privacy
- State Health Insurance Marketplaces
- Electronic Health Records
- Privacy of federal and state workforce databases
- Stalker apps

Critical IT Systems & Infrastructure
- Sector Specific Agencies
- NIST Cybersecurity Framework
- Vehicle Cybersecurity
- Internet of Things
- NCCIC

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

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

- Mandated Report
- HHS Components (FDA, CDC, NIH)
- High Impact Systems (NASA, NRC, OPM, VA)
- Cyber Risk Management
- National Mediation Board
Ongoing and Planned Work – Emerging Issues

- National Cybersecurity Protection System (Einstein)
- Healthcare.gov Data Hub
- CISO Authorities
- FedRAMP
- Continuous Monitoring
- DHS Cybersecurity Workforce
Ongoing and Planned Work – Consolidated Financial Statements

• IRS
• BFS / Federal Reserve
• FDIC
• SEC
• FHFA
• CFPB
• TARP
• SOSI
• DOD Statements of Budget Activity (Army, Navy, AF)
• OIGs
Ongoing and Planned Work – Critical IT Systems & Infrastructure

- Sector Specific Agencies
- NIST Cybersecurity Framework
- Vehicle Cybersecurity
- Internet of Things
- National Cybersecurity and Communications Integration Center
Ongoing and Planned Work – Privacy-related

- State Health Insurance Marketplaces (CA, KY, VT)
- Electronic Health Records
- Privacy of Federal and State Workforce Databases
- Stalker Apps
1. Does your agency currently have the capability to successfully implement CDM? Will it be an improvement over current continuous monitoring activities at your agency?
Sense of the Information Security Community

2. Are you currently where you need to be regarding implementation of PIV cards or other multi-factor authentication?
3. Was this summer’s cybersecurity sprint a useful exercise for improving information security at your agency?
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-15-725T, Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies (June 2015)
Recent GAO Reports

Recent GAO Reports

Questions
Contact

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