VA and Other Federal Agencies Need to Address Significant Challenges

GAO Update to:

The Information Security and Privacy Advisory Board

December 4, 2019
About the Report: GAO-20-256T

- Presented as testimony before HVAC Subcommittee on Technology Modernization
- Summarized status of information security across CFO Act agencies and at VA
- Based largely on prior GAO work
- Reviewed relevant OMB, IG, and agency reports
Background

- Federal law and policy set requirements for securing federal systems and information:
  - FISMA
  - E.O. 13800
  - NIST Cybersecurity Framework
- Civilian CFO Act agencies have spent billions on IT security related activities in FY 2018
- Federal agencies continue to report large numbers of security incidents, although VA has reported fewer incidents in recent years
Background – Federal information security incidents by threat vector, FY 2018

31,107 total information security incidents

- **Attrition**: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (8%)
- **Loss or theft of equipment**: The loss or theft of a computing device or media used by the organization (22%)
- **Web**: An attack executed from a website or web-based application (11%)
- **Email/phishing**: An attack executed via an email message or attachment (27%)
- **Impersonation**: An attack involving replacement of legitimate content/services with a malicious substitute (<1%)
- **External/removable media**: An attack executed from removable media or a peripheral device (31%)
- **Multiple attack vectors**: An attack that uses two or more of the attack types in combination (1%)
- **Improper usage**: Any incident resulting from violation of an organization’s acceptable usage policies by an authorized user that is not reported as part of another threat vector category (4%)
- **Other**: An attack method does not fit into any other type or is unidentified (1%)

Background – VA information security incidents by threat vector, FY 2018

1,776 total information security incidents

- Improper usage: < 1%
- External/removable media: < 1%
- Web: 4%
- Attrition: < 1%
- Impersonation: 41%
- Email/phishing: 20%
- Other: 20%
- Loss or theft of equipment: 13%

Source: GAO analysis of Office of Management and Budget data for fiscal year 2018. [GAO-20-256T]
Federal agencies, including VA, continue to have deficient information security programs

- IGs for 18 of 24 CFO Act agencies determined that their agency’s IS program was not effectively implemented during FY 2018

- IGs used a five-level maturity model to rate their agency’s IS policies, procedures, and practices related to the five core security functions – identify, protect, detect, respond, and recover – defined in NIST’s cybersecurity framework

- Level 4 (managed and measurable) and Level 5 (optimized) represent effective levels of security
IG ratings for five core security functions of 24 CFO Act agencies for FY 2018

Most CFO Act agencies had significant IS control deficiencies over financial reporting

- Agency IGs or IPAs reported for FY 2018:
  - 6 agencies w/ material weaknesses in IS controls
    - DOD, DHS, HUD, OPM, USDA, VA
  - 12 agencies w/ significant deficiencies
  - 6 agencies w/out significant deficiencies
    - DOE, DOI, DOJ, NRC, NSF, USAID

- IS was a major management challenge for 21 of 24 agencies
  - Not reported as a MMC for ED, NRC, NSF
Most CFO Act agencies had deficiencies in most IS control categories for their financial systems.

![Bar chart showing deficiencies in IS control categories.]

Source: GAO analysis of agency financial reports for fiscal year 2018. | GAO-20-256T
Most civilian CFO Act agencies, including VA, have reported meeting many cyber targets

<table>
<thead>
<tr>
<th>Key milestone</th>
<th>Performance Metric &amp; Target</th>
<th>Number of agencies reported meeting targets</th>
<th>VA status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software asset management</td>
<td>95% of software assets are covered by a whitelisting capability.</td>
<td>10</td>
<td>Not met</td>
</tr>
<tr>
<td>Hardware asset management</td>
<td>95% of hardware assets are covered by a capability to detect and alert upon the connection of an unauthorized hardware asset.</td>
<td>16</td>
<td>Not met</td>
</tr>
<tr>
<td>Authorization management</td>
<td>100% of high and moderate impact systems are covered by a valid security authorization to operate.</td>
<td>14</td>
<td>Not met</td>
</tr>
<tr>
<td>Mobile device management</td>
<td>95% of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised.</td>
<td>19</td>
<td>Met</td>
</tr>
<tr>
<td>Privileged network access management</td>
<td>100% of privileged users are required to use a Personal Identity Verification (PIV) card or Authenticator Assurance level 3 (AAL3) multifactor authentication method to access the agency's network.</td>
<td>18</td>
<td>Met</td>
</tr>
<tr>
<td>High-value asset access management</td>
<td>90% of high-value assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method.</td>
<td>14</td>
<td>Met</td>
</tr>
<tr>
<td>Automated access management</td>
<td>95% of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels.</td>
<td>15</td>
<td>Not met</td>
</tr>
<tr>
<td>Intrusion detection and prevention</td>
<td>At least 4 of 6 intrusion prevention metrics have met an implementation target of at least 90% and 100% of email traffic is analyzed using email authentication protocols that prevent malicious actors from sending false emails claiming to originate from a legitimate source.</td>
<td>8</td>
<td>Met</td>
</tr>
<tr>
<td>Exfiltration and enhanced defenses</td>
<td>At least 3 of 4 exfiltration and enhanced defenses metrics have met an implementation target of at least 90%.</td>
<td>23</td>
<td>Met</td>
</tr>
<tr>
<td>Data protection</td>
<td>At least 4 of 6 data protection metrics have met an implementation target of at least 90%.</td>
<td>16</td>
<td>Met</td>
</tr>
</tbody>
</table>
VA faces key security challenges as it modernizes and secures its IT systems

1. Effectively implementing information security controls
2. Adequately mitigating known security deficiencies
3. Fully establishing elements of a cybersecurity risk management program
4. Identifying critical cybersecurity staffing needs
5. Managing IT supply chain risks as part of IT modernization programs
Related GAO Reports

GAO contact information

- Di’Mond Spencer, Analyst-in-charge, SpencerD@gao.gov, 202-512-6684

- Greg Wilshusen, Director, WilshusenG@gao.gov, 202-512-6244
Questions