How to Best Protect Against Future Cyber Incidents

OMB Cyber and National Security Unit

August 26, 2015
Contents

- OMB Cyber Vision and Mission
- Recent Highlights
- Cyber Incident Trends
- Cybersecurity Sprint Immediate Actions
- Cybersecurity Sprint Strategy and Implementation Plan (CSSIP)
- Upcoming policies
- Questions
OMB Cyber Vision and Mission

- **Vision**: Reduce the number of cyber incidents where sensitive government information is compromised.

- **Mission**: Strengthen Federal cybersecurity through:
  1) Data-driven, risk-based oversight of agency and government-wide cybersecurity programs;
  2) Issuance and implementation of Federal policies consistent with emerging technologies and evolving cyber threats; and
  3) Oversight of the government-wide response to major cyber incidents and vulnerabilities to ensure appropriate mitigation measures are effectively implemented.
Recent Highlights

- Cybersecurity Sprint Successes
- 14 CyberStats in FY 2015
- Initiated FISMA Modernization implementation efforts
- Improving Cybersecurity Protections in Federal Acquisitions
- Circular A-130
FY 2014 Incidents

- The number of information security incidents reported to US-CERT increased approximately 15% from FY 2013 to FY 2014
- Increase in total information security events as well as enhanced capabilities to identify, detect, respond, and recover from these incidents
- FY 2014: 52% of Federal civilian cybersecurity incidents related to or could have been prevented by Strong Authentication implementation

<table>
<thead>
<tr>
<th>Reporting Source</th>
<th>Total Number of Incident Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Government Total</td>
<td>69,851</td>
</tr>
<tr>
<td>Federal Government: CFO Act</td>
<td>67,196</td>
</tr>
<tr>
<td>Federal Government: Non-CFO Act</td>
<td>2,655</td>
</tr>
<tr>
<td>Non-Federal</td>
<td>570,371</td>
</tr>
<tr>
<td>TOTAL</td>
<td>640,222</td>
</tr>
</tbody>
</table>

Source: FY 2014 OMB FISMA Report
CFO Act Agency Incidents

Cybersecurity Sprint Immediate Actions

- Scan networks for Indicators of Compromise (IOCs)
- Patch critical vulnerabilities without delay
- Tighten policies and practices for privileged users
- Implement Personal Identity Verification (PIV) cards for network access, especially for privileged users
- Identify high value assets and review corresponding security protections
Strong Authentication

CFO Act Agency Identity, Credential, and Access Management (Strong Authentication) Implementation
All Civilian Agency User Network Accounts (Privileged and Unprivileged)

Source: Agency reported data via CyberScope
Cybersecurity Sprint Strategy and Implementation Plan (CSSIP)

• **Prioritized Identification** and **Protection** of high-value information and assets

• **Timely Detection** and **Rapid Response** to cyber threats

• **Rapid Recovery** from incidents when they occur and accelerated adoption of lessons learned from these events

• **Retention** and **Recruitment** of the most highly-qualified cybersecurity workforce talent the Federal government can bring to bear

• **Efficient and Effective Acquisition** and **Deployment** of **Existing** and **Emerging Technology**
NIST CSSIP Collaboration

- OMB/NIST work on Cyber Sprint Strategy and Implementation Plan (CSSIP)
  - Existing and Emerging Technology (NCCOE)
  - Recovery Guidance
  - Cyber workforce mapping (NICE)
  - Assist agencies with standards/guidelines implementation
Upcoming Policies

• Cybersecurity Sprint Strategy and Implementation Plan (CSSIP)
• FY 2016 FISMA Guidance
• FY 2016 FISMA Metrics
• Improving Cybersecurity Protections in Federal Acquisitions
• Circular A-130
• ICAM Policy Updates
Questions?