Securing .gov with EINSTEIN 3 Accelerated (E³A)

April 19, 2016
The Cyber Threats

- Adversaries are persistent, breaking into USG computers and networks on a consistent basis.
- They use a variety of methods to gain access, disrupt services, and steal data

Vector of Malware Actions

- **Overall**
  - Direct Install: 74%
  - E-mail Attachment: 47%
  - Unknown: 10%
  - Web Drive-By: 8%
  - E-mail Link: 5%
  - Remote Injection: 3%
  - Downloaded by Malware: 2%

- **Small**
  - Financial: 84%
  - Espionage: 34%
  - Other: 8%

- **Large**
  - Financial: 58%
  - Espionage: 63%
  - Other: 6%

- “Overall” (all breaches of all organizations)
- “Small” (organizations with fewer than 1,000 employees)
- “Large” (organizations with 1,000 employees or more)
“EINSTEIN” is an operational moniker for the National Cybersecurity Protection System.

Analogy to security for a building:

- **E1** is the logbook, where guests sign their name, who they are visiting, and the time.
- **E2** checks the names in the logbook against a list of bad guys. If a bad guy enters or exits the building, it sounds the alarm.
- **E³A** is the gate and the guard that stops the bad guy from entering or exiting.
EINSTEIN Activity

• EINSTEIN 1 & 2 sensors see approximately 93% of .gov traffic.

  9,000,000,000
  Average number of flow records collected per day

  33,900
  Average number of alerts generated per day

• EINSTEIN 3 Accelerated protects approximately 47% of .gov users.

  1,000
  Average number of blocked traffic per day
NCPS (EINSTEIN) Program Benefits

Direct Agency Benefits

- Prevents cyber attacks from the most common and pervasive threat vectors
- Insight into network activities
- Reduces time to respond, remediate, and recover from cyber attacks
- Does not obligate agency funds

Enterprise Level Benefits

- Correlation of cyber activity across the .gov enterprise
- National threat data view to support cyber risk management
- Aggregate view of malicious activity patterns to better understand scope of attacks across the enterprise
Authorities


• Federal Information Security Management Act of 2002
  
  * OMB M-15-01 streamline agency reporting of information security incidents and requires agencies to entered into a legally sufficient MOA with DHS relating to the deployment of EINSTEIN

  
  * Need for expanded capabilities to address cyber threat

• Comprehensive National Cybersecurity Initiatives (CNCI)
  
  * Initiative #1 – TIC
  * Initiative #2 – IDS
  * Initiative #3 – IPSS