US-CERT
New Incident Notification Guidance

Ann Barron-DiCamillo
Director, US-CERT

June11th, 2014
Current Incident Process

- US-CERT and federal D/As employ a 6-category system for cybersecurity incident reporting
- System last updated in 2007, largely the same as in 1996
- The 2006-era categories conflate Effects (root access, denial of service) with Causes (malware, inappropriate usage).
  - Effect = Impact
  - Cause = Method (or Threat Vector)
- Results in large volumes of un-actionable information
  - Lack of impact data
  - Poor data quality
- Primary focus on incident categorization causes delay in notification
- NIST Special Publication 800-61 Revision 2 finalized
New Federal Incident Notification

What has changed:

- Replaced Categories with Threat Vectors
- Introduced Impact Classifications
- Moved root cause analysis to “closing” phase of the incident response process
- Eliminated “non-cyber” incidents from notification requirement
- Separate mandatory from voluntary notification
- Introduced a 1-hour notification timeframe for mandatory incidents
- Greater focus on coordination and bi-directional information sharing
- Changed paradigm from “reporting” to “notification”
Incident Notification Procedure

Are computer security policies, acceptable use policies, or standard computer security practices being violated or are under imminent threat of being violated?

Compromise of Confidentiality, Integrity, or Availability?
If no, identify threat vector and voluntarily report to US-CERT

Assess Recoverability
Identify Information Impact
Identify Functional Impact

If known, Identify Threat Vector
Provide Incident Details

Submit to US-CERT
Actions Taken

- August 2012, NIST SP 800-61 Revision 2 Finalized
- December 20th, 2013, Guidelines posted to OMB MAX Portal for comment
  - Received feedback from:
    - Department of Commerce (DOC)
    - Social Security Administration (SSA)
    - Department of Labor (DOL)
    - Department of Housing and Urban Development (HUD)
    - Department of State (DOS)
    - Department of Homeland Security (DHS)
    - Environmental Protection Agency (EPA)
    - Department of Health and Human Services (HHS)
- March 20th, 2014, updated Guidelines briefed at the ISIMC Meeting
- March 28th, 2014, updated Guidelines posted to OMB MAX Portal for comment
  - Received feedback from:
    - Department of Treasury (TREAS)
    - Department of Health and Human Services (HHS)
    - Environmental Protection Agency (EPA)
    - Department of Housing and Urban Development (HUD)
Common Concerns Addressed

- Guidelines do not account for non-cyber PII, conflicting with OMB Memorandum (M-07-16)
- Procedures for handling Classified incidents
- What is vs what is not notifiable
- Reporting timeframe
  - Detection vs Confirmation
  - 1 hour notification suggestion from impacted to top-level security center
  - Expand timeframe for specific incidents
- Application of impact classifications/threat vector to real world incidents
- Consideration for discretionary incident submissions
Schedule *(dates are tentative)*

- May 23rd 2014– Complete comment ingest/adjudication and finalize Guidelines
- June 27th 2014– Redraft current OMB M Series Memo to eliminate “non-cyber” incidents from the computer security incident notification requirement
- June 28th 2014– Configure internal systems to accept new notification framework
- October 1st 2014 – Complete development of US-CERT incident reporting web form to accommodate new reporting framework
- October 1st, 2015 – Final cutover to new threat vectors and impact classification per the new Guidelines
Questions

Ann Baron-DiCamillo, Director of US-CERT