From: **Burns, Sylvia** <sylvia_burns@ios.doi.gov>
Date: Mon, Jun 15, 2015 at 5:25 PM
Subject: Enhancing and Strengthening DOI's Cybersecurity Posture
To: DOI_ADIRs <DOI_ADIRs@ios.doi.gov>, DOI_BCISO <doi_bciso@ios.doi.gov>
Cc: ITT-ESC <itt_esc@ios.doi.gov>, DOI_Bureau_Heads <doi_bureau_heads@ios.doi.gov>, DOI_Deputy_Directors <doi_deputy_directors@ios.doi.gov>, "Kristen (Kris) Sarri" <kristen_sarri@ios.doi.gov>, Amy Holley <amy_holley@ios.doi.gov>, Elena Gonzalez <maria_gonzalez@ios.doi.gov>, Olivia Ferriter <olivia_ferriter@ios.doi.gov>, Kimberly Thorsen <Kim_Thorsen@ios.doi.gov>, Mary Pletcher <mary_pletcher@ios.doi.gov>

Colleagues - On Friday, June 12, 2015, the Office of Management and Budget (OMB) issued the below fact sheet regarding actions we need to take to strengthen our cybersecurity efforts. We have also developed several Department of the Interior (DOI)-specific immediate actions necessary to further protect our environment. This is one of a series of instructions targeted to continuously improve our cybersecurity posture.

I ask that you immediately begin implementing the following remediation activities:

1. Scan your network(s) for the Indicators of Compromise (IOCs) listed in the below Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) Analysis Report (previously provided). Prioritize Incidents 7 through 9.
    a. Use the enterprise IBM Endpoint Manager (IEM) and/or other security tools to scan network for IOCs; this is for IOCs with indicator type"MD5"
    b. Configure host- and network-based intrusion detection systems (HIDS/NIDS) to alert on activity related to IOCs; this is for IOCs with indicator type "IPv4", "Domain" and "Email"
    c. Configure network firewalls and other web and e-mail filtering systems to block access to IOCs with indicator type "IPv4", "Domain" and "Email"
    d. Configure local security information and event management (SIEM) tools to alert on activities related to IOCs

2. Comply with the Department of Homeland Security's (DHS) Binding Operational Directive (BOD) BOD-15-01 and the Secretary and Deputy Secretary's direction to patch **all** critical vulnerabilities on internal and external systems without delay. The vast majority of cyber intrusions exploit well known vulnerabilities that are easy to identify and correct. Bureaus/Offices should take immediate action on any DHS Vulnerability Scan Reports received from the Enterprise Vulnerability Manager, Kris Caylor.

a. Focus on Good Cyber Security Hygiene
    i. Ensure all manufacturer default accounts are either removed or disabled and passwords changed
    ii. Ensure critical patches and updates are installed
    iii. Ensure all systems are monitored by anti-virus (AV) and malware detection
        1. Utilize the IEM solution to regularly monitor AV software remains installed and that AV signatures are current as part of your Continuous Monitoring process..
    iv. Perform regular vulnerability scanning within your environment
    v. Ensure appropriate network segmentation and access controls are in place
    vi. Provide regular communications to end users
        1. General Security Awareness
        2. Phishing Scams
        3. Protecting credentials and sensitive data

3. Limit Active Directory (AD) Credential Caching

a. Create and implement AD Group Policy to limit caching of credentials as follows:
    i. Servers = 0
    ii. Workstations = 0
    iii. Laptops = 2 (setting to less than 2 on laptops may cause problems supporting remote personnel)

4. Enhance Identity, Account, Authentication, Authorization, and Access Management
    a. Begin planning for PIV/2-Factor authentication at the application layer
    b. Force password reset for all user and elevated privilege accounts

c. Change all service account passwords; Implement policies/procedures for reset of service account passwords every 60 days. If the 60 day reset period poses a significant mission impact, please advise immediately.
d. Change all local machine administrator accounts; Recommend implementation of a system that will enforce unique passwords for individual systems (Office of the Chief Information Officer (OCIO) is evaluating Xceedium - please consult with OCIO regarding evaluation results and opportunities to acquire similar capability through the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program under a potential Phase 2 Delivery Order opportunity that is under consideration).
e. Review and reduce the number of elevated privilege accounts
    i. Domain Admins
    ii. Built-in Administrators Group
f. Configure SIEM or other local tools for increased monitoring of activities using elevated accounts
    i. Implement regular audit log review process for elevated accounts
    ii. Configure alerts for all activity (e.g., pass and fail events for all application and operating system level event types) using elevated privileges during off-hours, outside of maintenance windows, etc
g. Reset Kerberos ticket granting authority for all Bureau domains
    i. First, ensure patch MS14-068 is installed on all endpoints (Windows workstations and servers)
    ii. Follow this link to get the Microsoft script for resetting the Kerberos ticket. https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51
    iii. Information on Golden Ticket can be found at http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf
h. Immediately expedite enforcement of Personal Identity Verification (PIV)/2-Factor authentication
    i. Enforce PIV/2-Factor authentication for remote access (expressly rescind all two-factor authentication waivers and exceptions previously granted)
    ii. Enforce PIV/2-Factor authentication for users at the machine level using AD Group Policy
    iii. Enforce use of PIV/2-Factor Authentication for all regular and ***privileged*** users (OCIO implementing Xceedium)

5. Secure remote access methods such as 'Jump Box' configurations (A jump box is a specially secured computer that administrators log on to in order to gain access to other computers and administrate them).
    a. Privileged access on jump box system is not authorized
    b. Credential caching is not authorized
    c. Restrict internet browsing and applications/programs

6. Identify High Value Assets
    a. Identify critical data, systems, equipment, infrastructure, applications
        i. Assess current protections
        ii. Determine gaps
        iii. Develop necessary remediation plans

7. Implement Additional Requirement for Core Data Centers
    a. In consultation and cooperation with the Department's OCIO Information Assurance Operations Division (IAOD), acquire, deploy, install and configure FireEye sensor agents on all (including workstations and servers) assets that reside within the core data centers and configure all agents to report to the Department's Enterprise Fireeye Management Console. Jim Warren is the primary point of contact regarding this action.

Later this week, I will be sending out more information on our next steps. This will include regular status reporting and a data call to get additional details from each bureau and office regarding the areas described above. Your responses will be incorporated into an overall report on DOI's efforts, which will be shared with DOI leadership.

Thank you for your prompt attention. If you have questions about these instructions, please contact Al Foster at alvin_foster@ios.doi.gov.

Sylvia

P.S. - See related article at http://www.infoworld.com/article/2612700/security/-jump-boxes--improve-security--if-you-set-them-up-right.html

---

Sent: Friday, June 12, 2015 6:01 PM
Subject: FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

FOR IMMEDIATE RELEASE
June 12, 2015

FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity

Cyberspace touches almost every facet of society and connects people in ways never imagined. Rapidly emerging technologies have transformed economies and enhanced the ability of governments around the world to drive innovation and provide services and benefits to citizens. Yet, cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century. Technologies and systems of the past cannot keep pace with rapidly evolving and persistent cyber threats. That is why the Administration has led a broad strategy to combat cyber threats and strengthen the Federal Government's overall cybersecurity infrastructure.

In 2009, President Obama named the first Cybersecurity Coordinator and directed a comprehensive Cyberspace Policy Review to assess U.S. policies and structures for cybersecurity. Since then, the Administration has taken a number of aggressive actions to upgrade the Federal Government's technology infrastructure and protect government networks and information, implementing tools and policies in order to detect and mitigate evolving threats. And we have seen significant progress. Federal departments and agencies have implemented capabilities to better manage cyber vulnerabilities when they arise, and agencies are instituting new methods of conducting business like requiring employees to log-on to networks using privileged credentials, instead of other less secure means of identification and authentication. Still, recent events underscore the need to accelerate the Administration's cyber strategy and confront aggressive, persistent malicious actors that continue to target our nation's cyber infrastructure.

To further improve Federal cybersecurity and protect systems against these evolving threats, United States Chief Information Officer (CIO) Tony Scott recently launched a 30-day Cybersecurity Sprint. As part of the effort, the Federal CIO has instructed Federal agencies to immediately take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks.

Specifically, Federal agencies must:

- **Immediately deploy indicators provided by the Department of Homeland Security (DHS) regarding priority threat-actor Techniques, Tactics, and Procedures to scan systems and check logs.** Agencies shall inform DHS immediately if indicators return evidence of malicious cyber activity.
- **Patch critical vulnerabilities without delay.** The vast majority of cyber intrusions exploit well known vulnerabilities that are easy to identify and correct. Agencies must take immediate action on the DHS Vulnerability Scan Reports they receive each week and **report to OMB and DHS on progress and challenges within 30 days.**
- **Tighten policies and practices for privileged users.** To the greatest extent possible, agencies should: minimize the number of privileged users; limit functions that can be performed when using privileged accounts; limit the duration that privileged users can be logged in; limit the privileged functions that can be performed using remote access; and ensure that privileged user activities are logged and that such logs are reviewed regularly.

Agencies must report to OMB and DHS on progress and challenges within 30 days.

- **Dramatically accelerate implementation of multi-factor authentication, especially for privileged users.** Intruders can easily steal or guess usernames/passwords and use them to gain access to Federal networks, systems, and data. Requiring the utilization of a Personal Identity Verification (PIV) card or alternative form of multi-factor authentication can significantly reduce the risk of adversaries penetrating Federal networks and systems. **Agencies must report to OMB and DHS on progress and challenges within 30 days.**

In addition to providing guidance to agencies, Federal CIO Scott also established a Cybersecurity Sprint Team, to lead a 30-day review of the Federal Government's cybersecurity policies, procedures, and practices. The team is comprised of the Office of Management and Budget's (OMB) E-Gov Cyber and National Security Unit (E-Gov Cyber), the National Security Council Cybersecurity Directorate (NSC Cyber), the Department of Homeland Security (DHS), and the Department of Defense (DOD). At the end of the review, the Federal CIO will create and operationalize a set of action plans and strategies to further address critical cybersecurity priorities and recommend a *Federal Civilian Cybersecurity Strategy*.

Key principles of the *Strategy* will include:

- *Protect*ing *Data*: Better protect data at rest and in transit.
- *Improving Situational Awareness*: Improve indication and warning.
- *Increasing Cybersecurity Proficiency*: Ensure a robust capacity to recruit and retain cybersecurity personnel.
- *Increase Awareness*: improve overall risk awareness by all users.
- *Standardizing and Automating Processes*: Decrease time needed to manage configurations and patch vulnerabilities.
- *Controlling, Containing, and Recovering from Incidents*: Contain malware proliferation, privilege escalation, and lateral movement. Quickly identify and resolve events and incidents.
- *Strengthening Systems Lifecycle Security*: Increase inherent security of platforms by buying more secure systems and retiring legacy systems in a timely manner.
- *Reducing Attack Surfaces*: Decrease complexity and number of things defenders need to protect.

###

ATTACHMENT B