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.