THE WHITE HOUSE
Office of the Press Secretary

FOR IMMEDIATE RELEASE
July 9, 2015

FACT SHEET: Administration Cybersecurity Efforts 2015

From the beginning of his Administration, the President has made it clear that cybersecurity is one of the most important challenges we face as a Nation. In response, the U.S. Government has implemented a wide range of policies, both domestic and international, to improve our cyber defenses, enhance our response capabilities, and upgrade our incident management tools.

As the cyber threat continues to increase in severity and sophistication, so does the pace of the Administration's efforts. Included in this fact sheet are some of the achievements of this Administration in just the last six months. Since cybersecurity is about managing risk throughout the entire enterprise over the long-term, not through isolated, one-off actions, the Administration will continue to build on these efforts in the future.

Supported private sector efforts to improve cybersecurity

- **Gained commitments to address the challenge -** The Administration hosted the **White House Summit on Cybersecurity and Consumer Protection** at Stanford University on February 13, which brought together leaders from businesses throughout the economy, consumer and privacy groups, educators, students, law enforcement, and other government agencies. At the Summit, **over two dozen companies made commitments.** They have all started to act upon their commitments to share best practices, adhere to stronger security standards, use the Cybersecurity Framework of Standards and Best Practices to manage their cyber risk, share cyber-threat information, and adopt more secure payment technologies.

- **Spurred information sharing –** At the Summit, the President issued an **Executive Order to encourage the development of Information Sharing and Analysis Organizations** (ISAOs) to serve as the hubs for sharing critical cybersecurity information and promoting collaboration for analyzing this information both within and across industry sectors. The Department of Homeland Security (DHS) solicited public comments and is holding public workshops to inform the development of standards by a Standards Organization, which will be selected in the fall. At the same time, the private sector has been busy organizing its communities and forming ISAOs.
    - DHS is developing a system for the **automated sharing of cyber threat indicators** with the private sector and government. The design of this system incorporates privacy and civil liberties protections. DHS is already using the

system to send out indicators, and this fall it will begin to receive information. Interested companies can work with the National Cybersecurity and Communications Integration Center (NCCIC) to prepare their networks for the automated sharing of cyber threat indicators.

- Through the **Cyber Information Sharing and Collaboration Program** (CISCP), DHS has built a trusted environment for sharing cyber threat information with the private sector through formalized Cooperative Research and Development Agreements. As of July 2015, there are 125 of these agreements in place and DHS has already shared over 28,000 indicators with these partners since the program's inception. An additional 156 Agreements are currently in negotiation which will further expand DHS' communications reach.
- The National Cyber Investigative Joint Task Force (NCIJTF), along with other federal cyber centers and sector specific agencies, are leveraging FBI's **Cyber Guardian** system to improve the process of managing cyber threat reports and notifying companies that have been the target of malicious cyber activity. Through this effort, directed by E.O. 13636, the cyber centers have logged over 10,000 cyber threat reports to date and facilitated over 2,000 notifications so far this year.

- **Proposed new cybersecurity legislation –** In January, **the President sent Congress a new cybersecurity legislative proposal** that included **information sharing and data breach notification provisions.** In April, the House of Representatives passed two bi-partisan bills similar to the President's information sharing proposal. The Administration looks forward to working with both parties in the Senate as it moves a bill to the floor.

- **Enhanced public/private collaboration –** Even as we continue to promote the National Institute of Standards and Technology (NIST)-developed Cybersecurity Framework as a key method for managing cyber risk, Federal departments have expanded collaborative engagements with the private sector to build mutual understanding and improve cybersecurity.
  - The Treasury Department, working closely with the Financial Services Sector Coordinating Council, has led a series **of public-private tabletop exercises** designed to simulate cyber-incidents and identify key challenges for effective public-private response.
  - The Environmental Protection Agency (EPA) is holding a series of **cybersecurity workshops** for drinking water and wastewater treatment and distribution facilities. These workshops, hosted across the country in partnership with DHS and the Federal Bureau of Investigation (FBI), have focused on cybersecurity threats, vulnerabilities, incident response procedures, and best practices.

- The Department of Defense (DoD) and DHS will soon **open offices in Silicon Valley** to focus on technology, innovation, and cybersecurity. These offices will partner with technology companies and utilize emerging technologies to improve national security.
- DoD, DHS, Department of Commerce's NIST, and General Services Administration (GSA), have jointly conducted quarterly meetings of the **Software and Supply Chain Assurance Forum** (SSCA). This ongoing public-private partnership brings together technical and business leaders from the public and private sectors to share best practices and emerging opportunities related to the disciplines of software and hardware assurance and supply chain risk management.

- **Established partnerships to secure technology** – The Department of Commerce has launched two initiatives to strengthen cybersecurity in the hardware and software used in computers and on the Internet.

  - Building off earlier initiatives, the National Telecommunications and Information Administration (NTIA) is expanding their domestic multi-stakeholder model to promote **Stakeholder Engagement on Cybersecurity in the Digital Ecosystem.** Since good security starts with addressing vulnerabilities, NTIA has **initiated a multi-stakeholder process on vulnerability research disclosure**. Bringing together technology companies, security researchers, and other stakeholders will create an open, consensus-based forum to address needs of both vendors and researchers in improving security. Potential outcomes could include a set of high level principles that could guide future private sector policies, or a more focused and applied set of best practices for a particular set of circumstances.

  - NIST has created **the National Cybersecurity Center of Excellence** to partner with the private sector, academia, and other government agencies in order to find solutions to security problems inherent in technology. The center will produce generally available standards-based reference designs, templates, and example "builds," in order to reduce costs and complexities and enable companies in all sectors to use more secure technology.

- **Protected consumers –** Since 2011, the Administration has worked to make online transactions more secure for business and consumers alike. In implementing the National Strategy for Trusted Identities in Cyberspace (NSTIC), the Department of Commerce has worked with thousands of stakeholders to jump-start an identity ecosystem, providing consumers with more secure, convenient, and privacy-enhancing experiences on the Internet.
  - Fifteen NSTIC pilots have demonstrated the capability for a vibrant new market; and the Identity Ecosystem Steering Group will be releasing an

Identity Ecosystem Framework this year to deliver a baseline set of standards and policies to ensure interoperability of these credentials throughout the internet.

- Last October, the President announced the **BuySecure initiative**, directing the Federal Government to begin using the latest chip and PIN technology for its retail payments. As of June 2015, GSA has worked with the payment industry to issue over 463,000 EMV equipped charge cards to Federal employees. In a phased approach, 4 million debit cards used by recipients of Federal benefits through the Direct Express® program are transitioning to this technology. In addition, nineteen Federal agencies are currently transitioning to new payment terminals while others will make the transition later in the year.
- Earlier this year, the Federal Trade Commission launched a website, **identitytheft.gov**, as a new one-stop resource for identity theft victims, in order to streamline the reporting and remediation process with credit bureaus.

Enhanced Federal cybersecurity

- **Accelerated efforts to increase security on Federal networks –**
  - Last month, the Federal Chief Information Officer launched **a 30-day Cybersecurity Sprint** to accelerate progress made on enhancing the Federal Government's cybersecurity. The Sprint's preliminary reporting shows great progress in Federal agency efforts to further protect information and assets, and improve the resilience of Federal networks, including: patching critical vulnerabilities, leveraging tools to block high-risk indicators, tightening access for privileged users, and increasing the use of multi-factor authentication. Specifically,
    - Federal civilian agencies have increased multi factor authentication use for privileged users **by 20 percent within the first 10 days of the Sprint**. Several agencies have increased multi factor authentication use for privileged users **to 100 percent**.
    - DHS has scanned **over 40,000 systems** for critical vulnerabilities and it is increasing those numbers every day. Federal agencies are patching vulnerabilities as they are identified.
  - In addition to these immediate actions, OMB is leading several Interagency Cyber Sprint teams focused on improving Federal cybersecurity in the following areas:
    - Prioritized Identification and Protection of high-value and sensitive information and assets;
    - Rapid Identification of cyber threats and Timely Detection of and Response to cyber risks; and,
    - Recovery from incidents when they occur and Accelerated Adoption of lessons learned from these events.

- OMB will continue working with agencies to identify challenges, accelerate implementation of tools and capabilities to detect and thwart cyber threats, and work with partners in Congress and across private industry to ensure we have the latest resources and tools availability to strengthen the Federal Government's overall cybersecurity infrastructure.

- **Increased Cyber Emphasis Government-wide under the Federal Chief Information Officer** – The Federal CIO has established a dedicated cyber team, **E-Gov Cyber**, to enhance oversight of agency and government-wide cybersecurity programs; and work with key Federal cybersecurity stakeholders to ensure federal cybersecurity receive the heightened level of attention, oversight, and management deserving of a national security priority. As of June 2015, E-Gov Cyber has led government-wide incident response actions to rapidly mitigate new vulnerabilities, such as Heartbleed; accelerated assessments of agency's cybersecurity program and defenses, by over 200 percent from the previous year; and established a new, on-going critical vulnerability scanning program for public facing web sites across the government.

- **Adopted more secure technologies –** Later this summer, the Administration will release new strategies and policies to help agencies secure their networks. These policies will include a ***Federal Cybersecurity Civilian Strategy*** and guidance to improve cybersecurity protections in Federal acquisitions. From the development of additional shared services to the faster acquisition of the most current cybersecurity technologies, this guidance will further empower Federal agencies to modernize their IT systems and utilize the latest cybersecurity tools.

- **Deployed new capabilities** – In order to provide Federal agencies with better capabilities to monitor their systems and combat cyber-threats, DHS is accelerating the deployment of two initiatives.
  - Pending Congressional approval, DHS will **accelerate Phase 2 of the Continuous Diagnostics and Mitigation (CDM) program** to better secure the users of government computers. This phase of CDM will provide Federal agencies the tools to monitor the activity of their users, identify whether users have appropriate privileges, and detect unauthorized access to sensitive information in near-real-time. The first phase of CDM covered over 50 percent of Federal civilian executive branch personnel. Agreements are now in place to cover over 97 percent of Federal civilian executive branch personnel. By the end of fiscal year 2016, over 60 Federal civilian agencies will be covered by CDM.
  - DHS is **accelerating deployment of the EINSTEIN 3A** intrusion prevention system across the Federal Civilian Government. EINSTEIN 3A detects and blocks cybersecurity threats before they can impact Federal agencies. The system now covers 15 federal civilian executive branch departments and

agencies, a 20 percent increase over the past 9 months. DHS will award a contract to provide EINSTEIN 3A for all federal civilian agencies by the end of 2015.

- **Initiated a cross-agency effort to examine how the government conducts background investigations –** Beginning in 2004, the Federal government has engaged in a variety of reform efforts to improve background investigation and adjudication timeliness and the quality of information used to make security clearance, suitability, fitness and credentialing decisions. In light of recent events, we will re-examine these efforts and determine if further fundamental reforms to the security clearance process or actions to accelerate progress on existing initiatives should be considered. Over the next 90 days, the Suitability and Security Performance Accountability Council - an interagency group chaired by OMB and comprised of the Director of National Intelligence (DNI) and the Director of the U.S. Office of Personnel Management (OPM), in their respective roles as Security and Suitability Executive Agents and representatives of DoD, DHS, DoJ, FBI, DoE and others - will conduct a review of key questions related to information security, governance, policy, and other aspects of the security and suitability determination process, to ensure that it is conducted in the most efficient, effective and secure manner possible.

- **Improved safeguards for unclassified information –** While classified information obviously warrants stringent protections, certain unclassified data also requires heightened protections due to its sensitive nature, even when held outside the government. **In June 2015, the National Institute of Standards and Technology (NIST) released Special Publication 800-171**, which provided Federal agencies with recommended requirements for protecting the confidentiality of this kind of information. Going forward, Federal agencies will use these requirements in contracts or other agreements established between those agencies and non-Federal organizations.

- **Encouraged Development of the workforce –** The National Initiative for Cybersecurity Education (NICE) has focused on education, training, and workforce development to support the workforce required to meet our growing cybersecurity needs. NICE has worked with government and private sector organizations to develop the National Cybersecurity Workforce Framework to provide a standard lexicon for careers in this space, making it simpler for cybersecurity professionals to join the Federal workforce.
    - OMB is leading a **Federal cyber workforce effort** to define the current gaps of cybersecurity talent throughout the government and outline current Special Hiring Authorities that can be used to bring in additional cybersecurity professionals; develop guidance related to these authorities; and promulgate tools and best practices to improve cybersecurity hiring.

- On May 29, 2015, the President signed the HERO Act into law. This Act provides veterans access to DHS' **online cybersecurity workforce training program** and an opportunity to continue serving the nation in the Immigration and Customs Enforcement Homeland Security Investigation's fight against cybercrime. DHS has also expanded access to this training program for employees of state, local, tribal, and territorial governments.

Developed new policies and capabilities to identify, defend against, and counter malicious cyber actors

- **Increased situational awareness within the government –** In February, the President **directed the formation of the Cyber Threat Intelligence Integration Center (CTIIC)**. The CTIIC will serve as the national cyber threat intelligence center to "connect the dots" within government regarding malicious foreign cyber threats to the nation so that relevant departments and agencies are aware of these threats in as close to real time as possible.

- **Strengthened our national defense -** In April, the Secretary of Defense released the new ***Department of Defense Cyber Strategy*** to guide the development of the U.S. military's cyber forces and strengthen the United States' cyber deterrence posture. The Strategy, which is now being implemented, focuses on building the capabilities necessary to defend the nation from cyber-attacks of significant consequence, defend DoD networks, data, and systems; and provide cyber support to military operations and plans.

- **Developed a new tool for responding to cyber threats –** In April, the President issued Executive Order 13694, which authorizes the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose **financial sanctions on individuals and entities** whose malicious cyber-enabled activities have contributed to a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. In establishing this new policy, the Administration is creating a means of imposing economic costs against not just those that conduct cyber attacks, but those responsible for supporting, enabling, or ordering such attacks.

- **Enforced the law -** Over the last year, the Department of Justice and authorities around the world have **collaborated on precedent-setting operations** to take down criminal marketplaces on the dark web, to free hundreds of thousands of computers from criminals' control in the takedown of the Gameover Zeus botnet, and to bring a dozen high-level cybercriminals to the United States to face justice here. The Department is sharing best practices from its experience battling cybercrime with the private sector, available at cybercrime.gov.

- **Propose new cybercrime enforcement legislation –** In January, the President sent to Congress a new cybersecurity legislative proposal that included **modernization of law enforcement tools to fight cybercrime**. The Administration's proposal contains provisions that would increase the consequences for breaking the law and committing crimes online, including by reaffirming important components of 2011 proposals to update the Racketeering Influenced and Corrupt Organizations Act (RICO) so that it applies to cybercrimes.

Engaged Internationally

- **Increased cooperation with our international partners -** The President has also taken steps to strengthen America's global leadership on cyber issues. As part of visits from the leaders of Brazil, the Gulf Cooperation Council states, India, Japan, and the United Kingdom, the President deepened our partnerships with those countries on strategic cybersecurity matters:
    - **Brazil** agreed to: expand bilateral cooperation on cyber issues by convening this fall the second meeting of the U.S.-Brazil working group on Internet and Information and communications Technology in Brasilia; affirm support for the multi-stakeholder model of internet governance; work collaboratively in the lead-up to key events this fall, including the tenth Internet Governance Forum and the Ten-Year Review of the outcomes of the World Summit on the Information Society.
    - **The Gulf Cooperation Council (GCC)** states agreed to: consult on cybersecurity initiatives, share expertise and best practices on cyber policy, strategy, and incident response. The United States will provide GCC member states with additional security assistance, set up military cybersecurity exercises and national policy workshops, and improve information-sharing.
    - **India** agreed to: strengthen cooperation on cybercrime and cooperate on enhancing operational sharing of cyber threat information, examining how international law applies in cyberspace, and working together to build agreement on norms of responsible state behavior.
    - **Japan** agreed to: expand bilateral cooperation on cyber issues by convening in August the 3rd annual Japan-US Cyber Dialogue; affirm voluntary norms of state behavior in cyberspace during peacetime; increase information sharing about cyber incidents and threats; cooperate to protect critical infrastructure; and, engage within international fora.
    - **UK** agreed to: improve critical infrastructure cybersecurity, including through a joint-exercise; strengthen cooperation on cyber defense, including through CERT, intelligence community, and law enforcement cooperation; and, support academic excellence through a new Fulbright award and university-to-university exchanges.

- **Bolstered participation in regional and multilateral venues** – the Administration has secured regional and international commitments intended to strengthen international cyber stability:
    - As part of the **G7 Leaders Summit**, G7 countries agreed to launch a new cooperative effort on enhancing cybersecurity of the energy sector.
    - As part of its consensus report on recommendations for the international community on international security issues in cyberspace, the **United Nations Group of Governmental Experts** affirmed three U.S.-drafted norms of state behavior in cyberspace during peacetime.

- **Strengthened NATO's cyber defense capability –** DoD will increase its participation in cyber exercises and help prepare NATO and our Allies to meet emerging cybersecurity challenges through a new initiative to assist with developing cyber defense strategies, planning for critical infrastructure protection, and conducting cyber defense posture self-assessments.

- **Fostered international law enforcement cooperation –** In this fiscal year, the FBI Cyber Division has established three new permanent **Cyber Assistant Legal Attaché (ALAT)** positions in London, Ottawa, and Canberra, and added five new temporary positions. Cyber ALATs are embedded with foreign host nation law enforcement or intelligence agencies to facilitate information sharing, increase cooperation on investigations, and improve relationships with foreign partners. This collaboration and these partnerships will be further expanded in coming years. In fiscal year 2016, FBI will establish four additional positions.

- **Expanded cyber capacity building initiatives –** All countries can combat malicious cyber activity by effectively preventing and mitigating incidents within their jurisdictions. To develop international capacity, the Department of State is **funding an expanded set of cyber capacity building initiatives**, including Computer Security Incident Response Team (CSIRT) development projects, an upcoming cybersecurity and cybercrime training for Central African nations, and other projects as part of its role as a founding member of the Global Forum for Cyber Expertise.

###