October 30, 2015

M-16-04

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

Shaun Donovan
2015.10.30 14:22:10
-04'00'

Tony Scott
Federal Chief Information Officer

Anthony Scott
2015.10.30 14:05:55
-04'00'

SUBJECT: Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government

Executive Summary

Strengthening the cybersecurity of Federal networks, systems, and data is one of the most important challenges we face as a Nation. As a result, the Federal Government is bringing significant resources to bear to ensure cybersecurity remains a top priority. This includes strengthening government-wide processes for developing, implementing, and institutionalizing best practices; developing and retaining the cybersecurity workforce; and working with public and private sector research and development communities to leverage the best of existing, new, and emerging technology.

In furthering this mission, the Federal Chief Information Officer (FCIO) initiated a 30-day Cybersecurity Sprint on June 12, 2015. The Cybersecurity Sprint Team ("Sprint Team"), led by the Office of Management and Budget (OMB), was comprised of representatives from the National Security Council (NSC), the Department of Homeland Security (DHS), the Department of Defense (DoD), and other Federal civilian and defense agencies. The initial Sprint memo instructed agencies to implement a number of immediate high priority actions to enhance the cybersecurity of Federal information and assets. This Cybersecurity Strategy and Implementation Plan ("CSIP") is the result of the Cybersecurity Sprint, and incorporates progress reporting and corrective actions that are ongoing.

The CSIP is the result of a comprehensive review of the Federal Government's cybersecurity policies, procedures, and practices by the Sprint Team. The goal was to identify and address critical cybersecurity gaps and emerging priorities, and make specific recommendations to address those gaps and priorities. The CSIP will strengthen Federal civilian cybersecurity through the following five objectives:

1) **Prioritized Identification** and **Protection** of high value information and assets;
2) **Timely Detection** of and **Rapid Response** to cyber incidents;
3) **Rapid Recovery** from incidents when they occur and **Accelerated Adoption** of lessons learned from the Sprint assessment;
4) **Recruitment and Retention** of the most highly-qualified **Cybersecurity Workforce** talent the Federal Government can bring to bear; and
5) **Efficient and Effective Acquisition** and **Deployment** of **Existing and Emerging Technology.**

The CSIP is organized in the following manner:

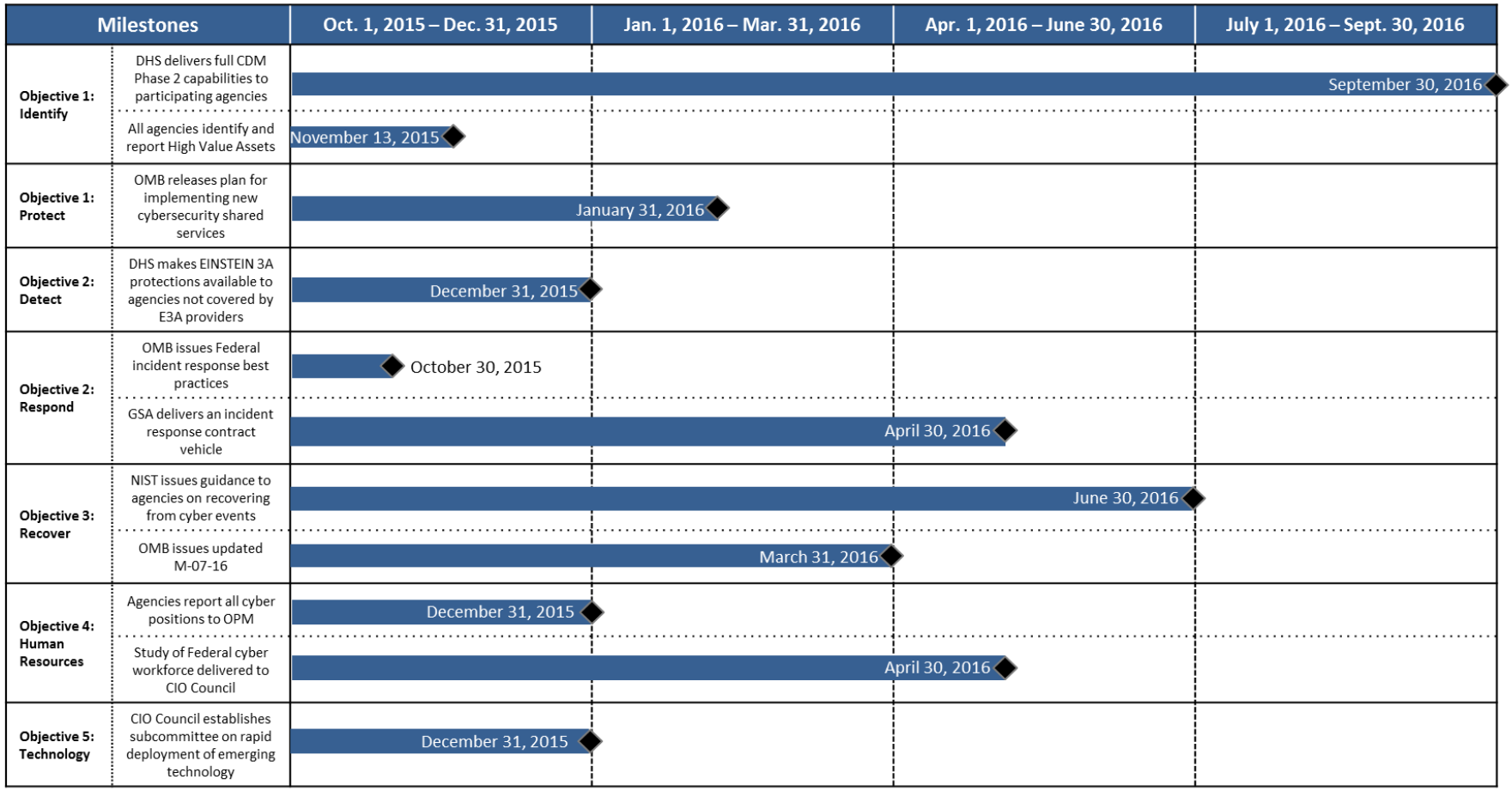
- **Objectives**: *"What we need to achieve"*
- **Actions**: *"How and where we focus our efforts to achieve those objectives"*

Specifically, the CSIP's key actions include:

- All agencies will continue to identify their high value assets (HVAs) and critical system architecture in order to understand the potential impact to those assets from a cyber incident, and ensure robust physical and cybersecurity protections are in place. The identification of HVAs will be an ongoing activity due to the dynamic nature of cybersecurity risks.
- DHS will accelerate the deployment of Continuous Diagnostics and Mitigation (CDM) and EINSTEIN capabilities to all participating Federal agencies to enhance detection of cyber vulnerabilities and protection from cyber threats.
- All agencies will improve the identity and access management of user accounts on Federal information systems to drastically reduce vulnerabilities and successful intrusions.
- OMB, in coordination with NSC and DHS, will issue incident response best practices for use by Federal agencies, incorporating lessons learned from past cyber incidents to ensure future incidents are mitigated in a consistent and timely manner. The best practices will serve as a living document to be continuously updated.
- The National Institute of Standards and Technology (NIST) will provide updated guidance to agencies on how to recover from cyber events.
- The Office of Personnel Management (OPM) and OMB will initiate several new efforts to improve Federal cybersecurity workforce recruitment, hiring, and training and ensure a pipeline for future talent is put in place.
- The Chief Information Officer (CIO) Council will create an Emerging Technology Sub-Committee to facilitate efforts to rapidly deploy emerging technologies at Federal agencies.
- The President's Management Council (PMC) will oversee the implementation of the CSIP in recognition of the key role Deputy Secretaries play in managing cybersecurity within their agencies.
- CIOs and Chief Information Security Officers will also have direct responsibility and accountability for implementation of the CSIP, consistent with their role of ensuring the identification and protection of their agency's critical systems and information.

The remainder of the CSIP outlines key actions, responsibilities, and timeframes for implementation. Progress will be tracked through several mechanisms, to include comprehensive reviews of agency-specific cybersecurity posture (CyberStats), the CIO Council, and the Information Security and Identity Management Committee (ISIMC). The PMC will serve as the Executive Steering Committee and will oversee quarterly performance reviews to identify major performance gaps.

CSIP Implementation – Key Milestones*



*Note: This timeline provides only a sampling of key actions and milestones outlined in the CSIP

Introduction

Strengthening the cybersecurity of Federal networks, systems, and data is one of the most important challenges we face as a Nation. Every day, the Federal Government experiences increasingly sophisticated and persistent cyber threats. While the Federal Government has prioritized its efforts to address these threats, several fundamental challenges exist which hinder progress in eliminating cybersecurity risks. Among these challenges is a broad surface area of legacy systems with thousands of different hardware and software configurations across the Federal Government, which introduces significant vulnerabilities and opportunities for exploitation. Additionally, each agency is responsible for managing its own information technology systems, which, due to varying levels of cybersecurity expertise and capacity, generates inconsistencies in capability across government.

The Federal Government is bringing significant resources to bear to ensure cybersecurity remains a top priority and agencies are held accountable for improving their performance in this critical area. These efforts include strengthening government-wide processes for developing, implementing, and institutionalizing best practices; developing and retaining the cybersecurity workforce; and working with public and private sector research and development communities to leverage the best of existing, new, and emerging technology.

To ensure that Federal agencies are dedicating appropriate attention and resources to address these critical and pressing challenges, the FCIO initiated a Cybersecurity Sprint on June 12, 2015. The Cybersecurity Sprint required agencies to take immediate steps to further protect Federal information and assets and improve the resilience of Federal networks. These actions included implementing strong user identity verification and authentication, patching critical vulnerabilities, scanning for cyber threat indicators, identifying critical information assets, and reviewing and reducing the number of privileged user accounts. In addition to providing direction to agencies, the FCIO established a Sprint Team to lead a 30-day review of the Federal Government's cybersecurity policies, procedures, and practices. Accordingly, the FCIO tasked the Sprint Team with creating and operationalizing a set of action plans and strategies to further address critical cybersecurity priorities and recommend a Federal civilian cybersecurity strategy. The result of those recommendations is the CSIP.

The CSIP directs a series of actions to improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of government assets and information, and further develop robust response and recovery capabilities to ensure readiness and resilience when incidents inevitably occur. The CSIP is part of a broader series of actions to bolster Federal civilian cybersecurity, which includes the issuance of updated guidance under the *Federal Information Security Modernization Act of 2014 (P.L. 113-283)* (FISMA); revisions to the Federal Government's governing document establishing policies for the management of Federal information resources: *Circular A-130, Managing Information as a Strategic Resource*; new guidance on implementing cybersecurity contracting language; cyber incident response best practices for use by Federal civilian agencies; the issuance of a blanket purchase agreement for Identity Protection Services designed to give Federal agencies ready access to best-in-class solutions and reduce wasteful and inefficient duplicative contracts for common-use services; and an updated Cybersecurity Cross-Agency Priority (CAP) Goal to improve Federal cybersecurity performance.

The CSIP emphasizes the need for a defense in depth[1] approach that relies on the layering of people, processes, technologies, and operations to achieve more secure Federal information systems. Inherent in a defense in depth approach is the recognition that all protection mechanisms have weaknesses that adversaries may exploit through several paths. Implementing the CSIP will not prevent every cyber incident. In fact, it is likely that agencies will discover additional and previously unknown malicious activity as they improve prevention and detection capabilities. Accordingly, the CSIP incorporates procedures to prepare agencies to respond to and recover from incidents, secure Federal information and assets, and ultimately strengthen their overall security posture.

The CSIP incorporates feedback from public and private sector subject-matter experts as well as lessons learned from current cyber incident response and recovery efforts affecting the Federal Government. The CSIP builds on existing policy work, including the Comprehensive National Cybersecurity Initiative (CNCI); Presidential Policy Directives; Executive Orders; legislation such as FISMA; OMB guidance; agency performance and incident data; and Federal Continuity Directives. The CSIP emphasizes the government-wide adherence to NIST standards and guidelines and builds on the core concepts of the *Framework for Improving Critical Infrastructure Cybersecurity*, which NIST developed in accordance with *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*.

Oversight

Responsibility for Federal Government cybersecurity is distributed and shared by all agencies; however, specific agencies have additional roles in supporting this mission and ensuring that the Federal Government has the tools, resources, and guidance necessary to make the risk-based decisions necessary to secure their systems. FISMA states that OMB oversees Federal agency information security policies and practices. The OMB Cyber and National Security Unit (OMB Cyber) was created at the beginning of FY 2015[2] to strengthen Federal cybersecurity through:

1) Data-driven, risk-based oversight of agency and government-wide cybersecurity programs;
2) Issuance and implementation of Federal policies to address emerging IT security risks; and
3) Oversight of the government-wide response to major incidents and vulnerabilities to reduce their impact on the Federal Government.

Progress on CSIP implementation will be tracked through several mechanisms, to include the PMC, comprehensive reviews of agency-specific cybersecurity posture (CyberStats), the CIO Council and the ISIMC. The quarterly performance reviews will be used to identify major performance and policy gaps, which will be addressed through regular engagement with agency leadership and future FISMA guidance. Additionally, OMB and NSC will work within the

[1] NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, defines defense in depth as: "information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization."

[2] OMB launched this dedicated unit within the Office of E-Government & Information Technology, also referred to as the Office of the Federal Chief Information Officer, in the Fiscal Year 2014 Federal Information Security Management Act Report to Congress.

interagency to ensure government-wide input and engagement on the creation of usable, targeted policies and guidance to help agencies continue to strengthen their cybersecurity posture.

The CSIP will strengthen Federal civilian cybersecurity through the following five objectives:

1) **Prioritized Identification** and **Protection** of high value information and assets;
2) **Timely Detection** of and **Rapid Response** to cyber incidents;
3) **Rapid Recovery** from incidents when they occur and **Accelerated Adoption** of lessons learned from the Sprint assessment;
4) **Recruitment and Retention** of the most highly-qualified **Cybersecurity Workforce** talent the Federal Government can bring to bear; and
5) **Efficient and Effective Acquisition** and **Deployment** of **Existing and Emerging Technology.**

The CSIP implementation described herein is organized in the following manner:

- **Objectives**: *"What we need to achieve"*
- **Actions**: *"How and where we focus our efforts to achieve those objectives"*

I. Objective 1: Prioritized Identification and Protection of High Value Information and Assets

Identify

To protect Federal Government information and assets, agencies must first identify the value and impact of the information on their systems and networks. Agencies must also identify the IT assets used to store, process, and transmit that information. Further, agencies must identify those assets and capabilities that enable mission essential functions and ensure delivery of critical services to the public.

Accordingly, OMB directed agencies to initiate processes to identify their High Value Assets (HVAs) at the beginning of the Cybersecurity Sprint. Agencies were to review and improve the security practices and controls around their HVAs. To assist agencies with this process, the Sprint Team developed a working definition of "high value asset"[3] and a list of attributes to consider when determining whether an asset, dataset, or repository is of high value. *Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*, also provides relevant guidance and requires Federal agencies to categorize their information and information systems to determine the worst-case adverse impact to operations and assets, individuals, other organizations, and the Nation if their information or systems are compromised.[4] The effort to identify HVAs builds on FIPS 199 and seeks to implement lessons learned from cyber incidents involving personally identifiable information (PII), by asking agencies' to give special consideration to the capability, intent, and specific targeting of high value data repositories by potential or actual adversaries.

Going forward, OMB is directing the following actions to prioritize the identification and protection of high value information and assets:

a. The Director of National Intelligence (DNI) will identify the appropriate interagency resources to lead a threat assessment of Federal HVAs that are at high-risk of targeting by adversaries **by December 31, 2015**. DHS will simultaneously lead a team, augmented by DoD, the Intelligence Community (IC), and other agency resources as needed, to continuously diagnose and mitigate the cybersecurity protections around the HVAs identified during the Cybersecurity Sprint. The DHS-led team will continue to conduct proactive assessments on a rolling basis as the IC, law enforcement, and other Federal entities identify new threats. DHS and DNI will share the results of these assessments with the agencies, as necessary.

[3] "High Value Assets" refer to those assets, systems, facilities, data and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical Federal operations, or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government.

[4] FIPS Publication 199 defines three levels of potential impact (i.e., low, moderate, and high) on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

i. To facilitate this process, OMB will establish a requirement in the *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements* [5] for civilian agencies to identify and submit their list of HVAs to DHS for assessment.
ii. Agency leadership will direct their respective CIOs to engage and collaborate with DHS during these HVA assessments.
iii. To identify HVAs containing PII, the Senior Agency Official for Privacy for each agency shall initiate a review of their information technology systems that maintain PII. The Senior Agency Official for Privacy shall evaluate the sensitivity and quantity of the PII and recommend to the CIO and agency head, as appropriate, whether a specific system or systems should be added to the agency's list of HVAs.
iv. In addition, for each HVA and information technology asset identified, the Senior Agency Official for Privacy shall review the processes for protecting PII on the systems and ensure that the applicable Privacy Act systems of records notice(s) and privacy impact assessment(s) that covers a given HVA or information technology asset is current, accurately addresses risks to PII, and includes any steps taken to mitigate those risks.

b. Per *OMB M-14-03, Enhancing the Security of Federal Information and Information Systems* and *OMB M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, Federal agencies must accelerate the implementation of capabilities and tools to identify risks to their systems and networks, to include, but not limited to, DHS's CDM program. CDM addresses parts of each stated objective of the CSIP, and its implementation is fundamental to helping agencies develop a better understanding of the risks to their IT systems and networks through improved identification and detection of cyber threats. Through CDM Phase 1, DHS is deploying sensors and tools at agencies that will provide a more accurate picture of: 1) the inventory of hardware and software assets under management, and 2) the ongoing security posture of each of those assets. DHS purchased CDM Phase 1 tools and integration services for all participating agencies in FY 2015. Implementation of these tools will result in coverage for all Chief Financial Officer (CFO) Act agencies and over 97% of the Federal Civilian Government.

c. During the Cybersecurity Sprint, DHS identified the need to accelerate CDM implementation throughout Federal agencies and has since developed a plan to accelerate the deployment of CDM Phase 2. In the first quarter of FY 2016, DHS has begun purchasing tools to provide Phase 2 capabilities for participating agencies. This capability will help ensure all employees and contractors at covered agencies are using appropriately secure methods to access Federal systems. DHS is scheduled to provide Federal agencies with additional Phase 2 capabilities throughout FY 2016, with the full suite of CDM Phase 2 capabilities delivered **by the end of FY 2016**.

[5] This guidance will be issued concurrent with the CSIP. The guidance is referred to as the "FY 2016 FISMA Guidance" hereafter in this document.

Protect

Over the course of the Cybersecurity Sprint, Federal civilian agencies increased their overall use of strong authentication from 42 percent to 72 percent. Specifically, Federal civilian agencies increased use of strong authentication for privileged users from 33 percent to nearly 75 percent. Although there is no single method by which all cyber incidents can be prevented, improving the access management of user accounts on Federal information systems could drastically reduce current vulnerabilities. Privileged user accounts are a known target for malicious actors but can be protected by an existing, strong authentication solution: Personal Identity Verification (PIV) credentials. Implementing strong authentication PIV credentials, as directed in *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors* (HSPD-12) and *Federal Information Processing Standard (FIPS) 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors*, is a cost-effective and immediate action that agencies should take to drastically reduce their risk profiles. PIV credentials efficiently authenticate an employee's identity and reduce the risk of identity fraud, tampering, counterfeiting, and exploitation.

To build on the strong authentication progress made during the Cybersecurity Sprint, in FY 2016 Federal agencies should continue to target the Administration Cybersecurity CAP goal of 100% strong authentication for all privileged users and 85% strong authentication for unprivileged users. While impressive strides have been made in areas such as strong authentication implementation, there is still more work to do. For example, once agencies have identified and inventoried their HVAs and high value information technology systems, they must protect them with a variety of policies, processes, and tools, consistent with applicable OMB guidance and NIST standards. Effective protection activities can include reducing the attack surface and complexity of IT infrastructure; minimizing the use of administrative privileges; utilizing strong authentication credentials; safeguarding data at rest and in-transit; training personnel; ensuring repeatable processes and procedures; adopting innovative and modern technology; ensuring strict domain separation of critical/sensitive information and information systems; and ensuring a current inventory of hardware and software components.

Furthermore, the employment of shared services is a proven approach for providing agencies with access to robust capabilities and can result in improved consistency and security across the Federal Government. They can also encourage the common application of standardized best practices, reduce costs and increases efficiencies. The Cybersecurity Sprint Team performed a Federal-wide inventory and assessment of current cyber-focused shared services. The Sprint Team assessed the maturity and effectiveness of these offerings, identified service gaps, and proposed additional offerings to address critical needs.

The CSIP initiates the following protection activities to improve Federal cybersecurity. These actions are in addition to those already being undertaken by Federal agencies and do not preclude agencies from continuing complementary work to secure their systems.

a. Tighten privileged user policies, practices, and procedures.
    i. The Cybersecurity Sprint Team required agencies to immediately review policies and practices for privileged users. Agencies should continue to:
        - inventory and validate privileged account scope and numbers;
        - 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 regularly reviewed.

b. Complete PIV implementation for all employees and contractors[6] required to obtain a PIV.
    i. The Cybersecurity Sprint directed agencies to immediately implement PIV for the following targets:
        - 100% of privileged users.[7]
        - 75% of non-privileged users.[8]
            a. The CAP Goal for FY 2016 Q1 is 85% of non-privileged users.
    ii. To facilitate this process, the Cybersecurity Sprint Team developed a compilation of best practices for PIV implementation and posted the collection on the CIO Council's Knowledge Portal.
    iii. Where necessary, GSA, in coordination with OMB, DHS, and DOD, and in consultation with NIST, will deploy technical resources for defined periods to assist agencies with remaining PIV implementation challenges.
    iv. The CSIP directs NIST to publish best practices for privileged user PIV implementation based on lessons learned from the Sprint **within 30 days.**[9]
    v. OPM, in coordination with NIST, OMB, and GSA, will update guidance on foreign nationals with regards to HSPD-12 applicability **by December 31, 2015.**

c. Address all critical vulnerabilities[10] and scan for Indicators of Compromise.
    i. Moving forward and on a rolling basis, the CSIP requires agencies to scan for indicators of compromise within 24 hours of receipt of the indicators from DHS.

---

[6] As defined by OMB Memorandum M-05-24: Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for Common Identification Standards for Federal Employees and Contractors.

[7] A network account with elevated privileges which is typically allocated to system administrators, network administrators, DBAs, and others who are responsible for system/application control, monitoring, or administration functions. – 2015 FISMA Metrics

[8] An unprivileged network account is any account that is not a privileged network account. – 2015 FISMA Metrics

[9] All instances of "within X days" in the CSIP means the deadline for the action is "within X days of the CSIP's issuance."

[10] The DHS National Cybersecurity Assessments and Technical Services (NCATS) team identifies critical vulnerabilities at agencies and assigns a severity score based on an industry-standard scoring model. For further questions contact ncats_info@hq.dhs.gov.

ii. Consistent with DHS's Binding Operational Directive 15-01, *Critical Vulnerability Mitigation Requirements for Federal Civilian Executive Branch Departments' and Agencies' Internet-Accessible Systems*, the CSIP directs agencies to patch all critical vulnerabilities immediately or, at a minimum, **within 30 days of patch release**. Vulnerabilities existing longer than 30 days will be included in agency PMC reports.

d. NSC and OMB will release the *EO 13681, Improving the Security of Consumer Financial Transactions* Implementation Plan **by December 31, 2015,** to require implementation of strong authentication and effective identity proofing for government digital services that make personal data accessible to citizens online.

e. Drawing on the work of the Sprint Team, OMB will release a plan for implementing new cybersecurity shared services **within 3 months**. These services will augment or supplement existing agency services, while providing new services for agencies without existing capabilities. Potential service offerings could include, but are not limited to:
   i. Identity, Authentication, and Authorization Services:
      - Agencies' ability to further their mission and achieve efficiencies by placing high value services online requires them to be able to have confidence in the identities of users accessing these services. This set of shared identity services could enable agencies to access digital credentials based on effective identity proofing methodologies and user-friendly strong authentication technologies. In addition, agencies can obtain validated information to support authorization decisions so that appropriate users can access their resources or benefits.
   ii. Mobile Security Services:
      - Mobile devices have become as powerful and connected as desktop and laptop computers, requiring the same level of attention to cybersecurity. Mobile security has unique challenges that require different solutions than existing programs offer. This service (or services) could address authentication, application management, device management, and encryption, and may include approved tools, best practices, and implementation support.
   iii. Network Segmentation Services:
      - Effective network segmentation management requires consistent application of best practices to limit lateral movement across networks. This shared service could provide network segmentation shared service capabilities across the Federal Government to help ensure that agencies consistently apply best practices to this complex management task. If operationalized, all Federal organizations would be asked to provide recommendations to the network segmentation services management offering to guide the proper implementation of network segmentation within an organization.
   iv. Digital Rights Management:
      - A digital rights management (DRM) shared service capability could enable a systematic approach to data-level protection across the Federal Government

and help prevent unauthorized review, redistribution, and modification of sensitive Government information. While protections at the network level remain essential, adding protection at the data level is critical to achieving defense in depth.

v. Encryption Services:
   - Encryption as a shared service could help ensure consistent application of security policies and potentially provide delivery of a range of cryptographic capabilities. If operationalized, this shared service could also leverage, and may require updates to the existing Federal Public Key Infrastructure (PKI). Proposals for this service offering may also include new requirements for employing web encryption (HTTPS), digitally signed email, and default encryption for sensitive information held by Federal civilian agencies.

II. Objective 2: Timely Detection of and Rapid Response to Cyber Incidents

Detect

The Sprint Team found that Federal civilian agency threat-detection capabilities have improved significantly in recent years. With DHS's EINSTEIN program providing network perimeter protection and the CDM program providing ongoing awareness of assets and activities within the network, agencies deploying these capabilities are now in a stronger position. Agencies have also made great strides in their efforts to share and receive cyber threat information, both with other agencies and the private sector, which allows network defenders to detect and block cyber intrusions before they cause damage. This section of the CSIP identifies further improvements that OMB, DHS, and Federal agencies will take to enhance information sharing efforts, detect cyber threats in real time, and rapidly respond to cyber incidents.

a. For agencies to deploy strong perimeter protections, DHS will build on the current EINSTEIN platform to implement advanced protections beyond the current signature-based approach. DHS has initiated the following efforts to advance the EINSTEIN program:
    i. DHS is piloting behavioral-based analytics to extend beyond the current approach of using known signatures and begin identifying threat activity that takes advantage of zero-day cyber intrusion methods. DHS is examining technologies from the private sector to evolve to this next stage of network defense. DHS will share lessons learned from the pilot study and next steps with OMB **by March 31, 2016**.
    ii. DHS has issued a contract action that will provide EINSTEIN 3A protections to participating agencies that are not covered by the ISPs currently under contract. This contract will make certain EINSTEIN 3A protections (e-mail and domain name system) available to all Federal Civilian Government agencies **by December 31, 2015**.

b. Agencies rely on protections deployed through their trusted internet connection (TIC) or Managed Trusted Internet Protocol Services (MTIPS) providers. OMB Cyber, in coordination with DHS, will initiate a 30-day review of current TIC architecture and baseline controls upon release of the CSIP with a focus on:
    i. Continuous agency review of their public-facing Internet connections for consolidation and reduction.
    ii. Ensuring all possible traffic, including mobile and cloud, goes through a TIC.
    iii. Options for where TICs can be hosted to improve bandwidth coverage.
    iv. Additional tools that can be implemented at a TIC location.
    v. How external vendors who store, process, and transmit agency data for or on behalf of the government can have their traffic securely encapsulated within the TIC connectivity.

c. The CSIP emphasizes ways to advance Federal-wide information sharing on critical vulnerabilities and threats, indicators of compromise, and best practices. Information sharing is essential not only for detecting and blocking intrusions on a specific targeted

organization, but for understanding the broader landscape of cyber risk. DHS analyzes cybersecurity information from sensors deployed across the Federal Government and from incidents reported by Federal agencies and the private sector. With this information, DHS is able to identify when adversaries appear to be targeting particular sectors or types of organizations and share the information proactively, helping agencies understand emerging risks and develop effective protective measures to block threats before incidents occur.

i. One primary barrier to effective information sharing is a lack of operational speed. Information sharing must be sufficiently rapid to detect and block threats before targeted networks are adversely impacted. The DHS National Cybersecurity and Communications Integration Center (NCCIC) has developed an automated system to share cyber threat indicators in near real-time and is working aggressively to build this capability across government and out to the private sector. The CSIP directs all CFO Act agencies to work with DHS to implement automated indicator sharing by developing their own capability, procuring commercially available solutions, or participating in a shared service, once available, **within 12 months**.

d. **Beginning in FY 2016**, GSA will develop a Business Due Diligence Information Service that will provide agencies with a common government-wide capability for identifying, assessing, and managing cyber and supply chain risk throughout the acquisition process.

Respond

The Sprint Team identified several common challenges during the Cybersecurity Sprint and determined that Federal Civilian Government cyber incident response procedures and practices are not consistently documented or implemented. As instances of cyber incidents simultaneously affecting multiple Federal agencies are likely to increase, the Federal Government requires streamlined response efforts and enhanced procedures for communication and coordination. The CSIP aims to address these challenges through the creation of incident response best practices for Federal civilian agencies. This new guidance will help set expectations across all involved parties and ensure consistency across incident response efforts while remaining flexible enough to guide activities under various conditions and situations.

The CSIP addresses this challenge by initiating the following actions:

a. OMB, in coordination with NSC and DHS, will provide Federal civilian agencies with incident response best practices along with the FY 2016 FISMA Guidance, which will be issued concurrent with the CSIP, to provide a reference guide for responding to major incidents[11] affecting Federal civilian agencies. The best practices will address several common challenges identified during the Sprint by formalizing the role of an on-scene coordinator, assigning incident response work streams, and establishing entry and exit criteria for the response phase. Furthermore, the best practices will clarify existing requirements for agencies to notify US-CERT, Congress, and victims of a cyber incident;

[11] For a definition of major incidents, please see the FISMA FY 2016 Guidance.

will help improve agency plans and procedures to ensure that relevant authorities are documented and understood; and will enhance inter-agency communication and coordination procedures to ensure incidents are mitigated appropriately and in a timely manner.

b. In the FY 2016 FISMA Guidance, OMB will require that all departments and agencies (not bureaus or components) designate one principal Security Operations Center (SOC), or equivalent organization to be accountable to agency leadership, DHS, and OMB for all incident response activities. Agencies will provide this information to US-CERT **by November 13, 2015**.

c. Separately, **within 3 months**, OMB, in coordination with DHS, will provide agencies with best practices and use cases for Federal SOCs to ensure consistent roles, responsibilities, policies, and procedures are employed by SOCs across the Federal Government.

d. In the FY 2016 FISMA Guidance, OMB will require agencies to have a standing Federal Network Authorization with DHS to ensure DHS can rapidly deploy on-site resources to conduct incident response activities, when necessary. The authorization should be reviewed on a semi-annual basis and remain on file with DHS.

e. The CSIP directs GSA, in coordination with OMB, to research contract vehicle options and develop a capability to deploy incident response services that can quickly be leveraged by Federal agencies, on a reimbursable basis. The incident response service will be managed by the contracting agency, in coordination with DHS and OMB. GSA will develop requirements and deliver a detailed implementation plan for this task to OMB **within 3 months;** then complete the acquisition process and deliver the final capability **within 6 months**.

III. Objective 3: Rapid Recovery From Incidents When They Occur and Accelerated Adoption of Lessons Learned From The Sprint Assessment

Recovery

The CSIP defines "recover" as the development and implementation of plans, processes, and procedures for recovery and full restoration, in a timely manner, of any capabilities or services that are impaired due to a cyber event. The Cybersecurity Sprint identified that Federal-wide and agency-specific policies and practices for recovering from cyber events are inconsistent and vary in degree of maturity. In recent years, the Federal Government has prioritized protecting its assets and detecting threats. As an increasing number of threats are detected, the Federal Government must begin to improve both its response and recovery capabilities. Recent events have demonstrated the need for policies or plans related to recovery from cyber events to remain flexible to better allow agencies to respond to and recover from evolving and sophisticated threats.

To date, there have been a number of Federal-wide policies and standards that provide guidance as to how agencies should recover from cyber events. For example, the *NIST Cybersecurity Framework for Critical Infrastructure Cybersecurity* identifies "Recover", which includes the sub-categories of Recovery Planning, Improvements, and Communications, as one of its primary Functions. Additionally, numerous controls within *NIST Special Publication 800-53 Revision 4* address elements of recovery controls and capabilities that agencies should address. OMB also published *OMB M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, which provides guidance to agencies as to how they should protect against data breaches and respond and recover when one occurs. Despite the existence of available standards and guidance, there remains room for improvement.

The CSIP initiates the following actions to help agencies rapidly recover from incidents when they occur and accelerate adoption of lessons learned from these events.

a. The CSIP directs NIST to provide guidance to agencies **by June 30, 2016,** on how to recover from a cyber event, focusing on potential scenarios to include, but not limited to, a data breach or a destructive malware campaign.

b. The CSIP directs OMB to update OMB M-07-16 **by March 31, 2016,** to reflect current best practices and recent lessons learned regarding privacy protections and data breach standards. This updated guidance regarding the collection and disposal of PII will help agencies ensure compliance with relevant laws and regulations for the protection of this sensitive information.

c. To complement these efforts, the CSIP also directs OPM **within 3 months** to review options and develop and deliver to OMB recommendations for making Identity Protection Services a standard Federal employee benefit.

IV. Objective 4: Recruitment and Retention of the Most Highly-Qualified Cybersecurity Workforce Talent the Federal Government Can Bring to Bear

Human Resources

Strengthening Federal cybersecurity is not possible without the appropriate talent. The Federal workforce must keep pace with the growing dependence on technology for mission essential activities. A well-functioning security organization requires a blend of technical, policy, legal, and leadership resources covering multiple disciplines within cybersecurity. A focus on any one skillset without an understanding of overall organizational needs can lead to failure. The Cybersecurity Sprint identified two key observations related to the Federal cybersecurity workforce: 1) the vast majority of Federal agencies cite a lack of cyber and IT talent as a major resource constraint that impacts their ability to protect information and assets; and 2) there are a number of existing Federal initiatives to address this challenge, but implementation and awareness of these programs is inconsistent. The CSIP initiates the following actions to address these challenges in recruiting and retaining a high-quality cybersecurity workforce. These initiatives will inform a broader Cybersecurity Human Resources Strategy to be published by OMB **within 6 months**, which will help ensure the Federal Government can recruit, develop, and maintain a pipeline of cybersecurity talent throughout the Federal Government.

a. The CSIP directs all agencies to participate in the following efforts:
    i. OPM and OMB will compile existing Special Hiring Authorities (by agency) that can be used to hire cybersecurity and IT professionals across government. OPM will clarify legal guidelines and provide guidance to agencies on how to increase the understanding of these Special Hiring Authorities, and how agencies should work with their human resources departments to implement them, where appropriate, and rapidly close talent gaps and accelerate hiring **by December 31, 2015**.
    ii. Agencies will participate in OPM's existing Special Cyber Workforce Project, which provides cybersecurity job codes by specialty, so that agency leadership can identify the universe of their cyber talent, understand Federal-wide challenges for retaining talent, and address gaps accordingly. Agency CIOs, working collaboratively with Chief Human Capital Officers, should use this assessment to identify their top five cyber talent gaps, which will be due to OPM and OMB **by December 31, 2015**.

b. The CSIP directs DHS to begin piloting their Automated Cybersecurity Position Description Hiring Tool across the Federal Government. DHS is also directed to develop and report on performance and adoption metrics so that agency leadership can better understand how to leverage the tool. Used in concert with relevant OPM Position Classification Standards, the tool will assist in the implementation of the National Initiative for Cybersecurity Education (NICE) Framework by consistently mapping the NICE job codes according to selected skills and KSAs (Knowledge, Skills and Abilities). The tool enhances cybersecurity workforce recruitment by decreasing the applicant time-

to-hire and by ensuring cybersecurity job announcements contain clear, technical content. DHS must also post their own internal Cyber Workforce Analysis results on the CIO Council Knowledge Portal **by November 30, 2015,** as a best practice for other agencies to leverage.

c. The CSIP directs OPM, DHS, and OMB, in coordination with NIST and other NICE partner agencies, to map the entire cyber workforce landscape across all agencies using the NICE National Cybersecurity Workforce Framework and identify cyber talent gaps and recommendations for closing them **within 6 months.** The mapping exercise and recommendation report should focus on:
    i. Existing employees and open positions, starting with the civilian agencies, this assessment should also consider contractor resources.
    ii. Existing resources and open positions within the DoD and the IC, this assessment should also consider contractor resources.
    iii. Changes to human resources processes and systems that not only incorporate best practices for retaining and incentivizing employees, but simplify and expedite the hiring process.
    iv. Capacity building actions to assist human resource professionals in their efforts to implement CSIP recommendations.
    v. Training and professional development opportunities for the existing workforce in order to address critical needs.
    vi. Leveraging the National Science Foundation CyberCorps® Scholarship for Service and the Advanced Technological Education program to help inform potential educational programs to help develop a pipeline of students from colleges, universities, and other providers.
    vii. Driving awareness of cybersecurity internship opportunities and programs that establish the possibility of hiring participants into permanent positions.
    viii. Creating and deploying "Tiger Teams" comprised of subject matter experts from across the Government to address critical workforce needs.

d. The CSIP also directs OPM, DHS, and OMB, in coordination with NIST and other NICE partner agencies, to develop recommendations for Federal workforce training and professional development in functional areas outside of cybersecurity and information technology that support cybersecurity efforts **within 6 months**. These recommendations should address, at a minimum, the following functional areas: legal counsel, budget, procurement, privacy, and civil rights and liberties.

V. Objective 5: Efficient and Effective Acquisition and Deployment of Existing and Emerging Technology

Existing/Emerging Technology

As stated above, the CSIP acknowledges the need for a defense in depth approach, or a layering of people, processes, procedures, and tools, to achieve a more secure Federal landscape. This section describes the steps the Federal Government must take to provide agencies with the appropriate technological toolset to adequately secure the functions, systems, and information enabling their missions. The Cybersecurity Sprint Team observed that the Federal Government has made strides in the incubation and adoption of emerging technology for cybersecurity purposes through innovation and incubator programs, to include the Defense Advanced Research Projects Agency's Information Innovation Office (I2O), the DHS Homeland Security Advanced Research Projects Agency (HSARPA), in particular the Transition to Practice (TTP) program, and the NSF Secure and Trustworthy Cyberspace (SaTC) Transition to Practice (TTP) program. Furthermore, Federal agencies have adopted existing commercially available off-the-shelf (COTS) technology through programs like EINSTEIN and CDM. In addition to these incubators, the NIST National Cybersecurity Center of Excellence (NCCoE) is a public-private partnership that fosters innovation and accelerates the adoption of secure technologies for the public and private sectors.

However, the connection between these programs and the agencies in need of existing and emerging technology must be strengthened. The Cybersecurity Sprint identified a need for a Federal-wide technology assessment followed by a comprehensive program to assist agencies with the procurement, assessment, certification and accreditation of existing and emerging technology. The CSIP initiates the following actions to address the challenge of acquisition and deployment of existing and emerging technology:

a. OMB, in coordination with NSC, and OSTP, will convene a working group comprising representatives, as appropriate, from DHS, GSA, NIST, DOD, and the CIO Council, to develop recommendations for strengthening and better coordinating the collective ability of Federal civilian departments and agencies to identify, acquire, and rapidly implement innovative commercially-available cybersecurity products and services. The working group will deliver its recommendations to the Federal CIO and NSC Coordinator for Cybersecurity **by March 31, 2016**.

b. The CSIP directs GSA to develop a procurement capability to allow Federal agencies to access the technology at any known Federal technology incubator, to include, but not limited to, the NCCoE, I2O, and DHS HSARPA **by December 31, 2015**.

c. The CSIP directs the Federal CIO Council to create an Emerging Technology Sub-Committee under the ISIMC **by December 31, 2015** that will be responsible for facilitating efforts to expediently deploy emerging technologies at Federal agencies. This group will provide requirements, challenges, and feedback to both incubators and agencies.

d. The CSIP directs GSA and DOE, in coordination with the Federal CIO Council, DOD, ODNI, DHS, and the NCCoE, to establish a working group that will identify and connect current testing environments for new technology solutions and submit recommendations for establishing new testing environment solutions to OMB **no later than December 31, 2015**. Additionally, GSA will establish formal protocols for agencies to utilize these shared testing capabilities and share results broadly for promising technology solutions with potentially broad applicability.

e. The CSIP directs the DHS CDM Program to work with the NCCoE to develop solutions and guidance related to CDM including providing technical guidance, best practices, sample implementation plans, and capability assessment methodologies **within 2 months**.

f. The CSIP directs the NCCoE, in addition to their existing priorities, to focus on derived credentials solutions and other strong authentication solutions for mobile devices as a critical component of a broader effort to improve mobile device management.