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

THE DIRECTOR

October 30, 2015

M-16-03

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

Shaun Donovan
2015.10.30
12:11:59 -04'00'

SUBJECT: Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements

Purpose

This memorandum establishes current Administration information security priorities and provides agencies with Fiscal Year (FY) 2016 Federal Information Security Modernization Act (FISMA) and Privacy Management reporting guidance and deadlines, as required by the *Federal Information Security Modernization Act of 2014*. In many cases, this memorandum establishes new guidance to address discrete challenges identified over the last fiscal year. This guidance is also designed to complement the specific requirements directed in the Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government (CSIP), which is being published in coordination with this memorandum and is described in further detail below.

This memorandum is directed to Federal Executive Branch agencies and does not apply to national security systems. Agencies operating national security systems, however, are encouraged to adopt the initiatives herein and abide by the spirit of this memorandum.

Background

The Federal Government has seen a marked increase in the number of information security incidents affecting the integrity, confidentiality, and/or availability of government information, systems, and services. These incidents demonstrate the need to strengthen information security practices, policies, and governance. In response to these persistent threats, the Office of Management and Budget (OMB), in coordination with the Department of Homeland Security (DHS) and the Department of Commerce's National Institute of Standards and Technology (NIST), has taken a number of critical steps to improve Federal information security, to include:

Federal Adoption of the NIST Cybersecurity Framework: In early FY 2015, OMB and the National Security Council (NSC) staff created a quarterly cybersecurity assessment organized according to the functions in the NIST Framework for Improving Critical Infrastructure

Cybersecurity (Identify, Protect, Detect, Respond, and Recover) and associated outcomes to comprehensively assess agency cybersecurity performance. The assessment builds on the existing foundation of FISMA metrics and the Cybersecurity Cross Agency Priority (CAP) goals and is reviewed by agency senior leadership. Moving forward, this assessment will be the cornerstone initiative for how OMB measures Federal agency cybersecurity performance.

Increased Focus on CyberStat Review Sessions: In FY 2015, the OMB Cyber and National Security Unit (OMB Cyber), part of the Office of E-Government & Information Technology, was created and completed double the number of agency CyberStat Review Sessions (CyberStats) compared to the previous fiscal year. CyberStats are evidence-based meetings led by OMB to ensure agencies are accountable for their cybersecurity posture, while at the same time assisting them in developing targeted, tactical actions to deliver desired results.

Addition of Privacy Program Review Sessions: Following publication of this guidance, OMB will be meeting with Federal agencies to conduct face-to-face, evidence-based reviews of the agencies' privacy programs. These reviews will allow OMB to more directly oversee select agencies' compliance with privacy requirements and assist the agencies in developing targeted plans for improving their privacy program management.

Implementation of the Cybersecurity Sprint: Initiated by the Federal Chief Information Officer (CIO), the Cybersecurity Sprint instructed Federal agencies to immediately take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks. Agencies were instructed to:

- Immediately deploy indicators provided by DHS regarding priority threat-actor Techniques, Tactics, and Procedures (TTPs) to scan systems and check logs;
- Patch critical vulnerabilities without delay;
- Tighten policies and practices for privileged users;
- Dramatically accelerate implementation of strong authentication, especially for privileged users; and
- Immediately identify agency specific High Value Assets (HVAs) and assess the security protections around those HVAs.

As a result of the effort during the Sprint, the Federal Government increased the use of strong authentication by 30% from 42% to 72%, for all civilian agency users. Federal agencies also reduced the amount of time required to scan for indicators of compromise and patch critical vulnerabilities.

In addition to these immediate operational steps, as part of the Cybersecurity Sprint, OMB established a team to lead a 30-day review of the Federal Government's cybersecurity policies, procedures, and practices. In coordination with the release of this memorandum, OMB will publish the results of this process in the form of the CSIP, which outlines a number of proactive measures the Federal Government will undertake over the next year to improve the state of Federal cybersecurity.

Review of Security in Contract Clauses: As a result of cyber incidents impacting Government information that resides on or is connected to contractor systems, a group of experts in security, privacy, and the Federal acquisition process were tasked with reviewing existing contract clauses and providing recommendations to improve cybersecurity protections in Federal acquisitions. The group's recommendations were used to inform the development of OMB guidance, titled *Improving Security Protections in Federal Acquisitions*. The guidance, to be released in the first quarter of FY 2016, provides clarity around requirements for security in Federal acquisitions.

Summary of Contents

Section I: Information Security and Privacy Program Oversight and Reporting Requirements
This section is comprised of requirements which will ensure agencies are adopting Administration priorities and providing OMB with the performance indicators necessary to conduct oversight. Furthermore, this section provides guidance to agencies on how to address requirements established in FISMA 2014. Specifically, this section:

- Provides Federal agencies with timelines and requirements for quarterly and annual reporting;
- Establishes detailed instructions for preparing the annual agency FISMA reports, which must be submitted to DHS through CyberScope **no later than November 13, 2015**; and
- Provides the definition of a "*Major Incident*".

Section II: Incident Response Coordination Activities
This section provides agencies with guidance regarding incident response coordination activities based upon the lessons learned from incidents that impact the Federal government in FY 2015. This section updates procedures to ensure greater consistency in agency response practices by: 1) requiring that agencies formally address the need for sensitive positions, 2) formalizing the process by which agencies can request on-site technical assistance from DHS, and 3) providing agencies with best practices based upon lessons learned from major cybersecurity incidents.

In addition to the sections referenced above, updates to the Frequently Asked Questions can be found at the following link: https://community.max.gov/x/eQPENw.

Section I: Information Security and Privacy Program Oversight and Reporting Requirements

The following section provides agencies with quarterly and annual reporting guidelines that serve two primary functions: 1) to ensure agencies are implementing Administration priorities and cybersecurity best practices, and 2) to provide OMB and DHS with the data necessary to perform relevant oversight and operational duties pursuant to FISMA 2014.

In early FY 2015, OMB and the NSC staff established an assessment to provide agencies with a method for conducting risk-based cybersecurity assessments, manage various policy requirements, and engage with senior leadership on cybersecurity priorities. This assessment measures agency performance towards the implementation of existing FISMA (to include Cybersecurity CAP goal) metrics, OMB guidance, NIST standards, and cybersecurity best practices. The assessment formally adopts and is organized according to the functions in the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover) and associated outcomes as the basis for comprehensively assessing agency cybersecurity performance. Moving forward, agencies will be required to conduct these assessments on a quarterly basis, based upon the schedule outlined below.

In order to reduce the reporting burden on agencies, OMB consolidated its cybersecurity-related information collections. Starting in FY 2016, agencies will be able to report the majority of their cybersecurity performance information through CyberScope.

To further clarify reporting for agencies, the term "Micro agency" will no longer be used and those agencies formerly referred to as Micro agencies will be considered Small agencies. This and future guidance will be focused on requirements for Chief Financial Officer (CFO)[1] Act agencies and Small agencies.

Reporting Requirements and Deadlines

Federal agencies shall adhere to the following reporting requirements and timelines:

FY 2015 Annual FISMA Reporting Deadline

Annual FISMA Report:	**All agencies will update the Annual FY 2015 FISMA metrics by November 13, 2015.** **While agencies must submit their data to OMB by November 13, 2015, their Agency reports are due to Congress by March 1, 2016.**

[1] 31 USC 901 http://www.gpo.gov/fdsys/granule/USCODE-2011-title31/USCODE-2011-title31-subtitleI-chap9-sec901/content-detail.html

	All agencies, to include Small and independent agencies, should complete the Chief Information Officer (CIO), Inspector General, and Senior Agency Official for Privacy questions in DHS's CyberScope no later than November 13, 2015.

FY 2015 Agency Reports to OMB and Congress

In accordance with FISMA 2014 (Section 301, 44 U.S.C § 3554), agencies shall submit an annual report to OMB, DHS, and the appropriate committees.

Agency Letter - An official letter, signed by the head of the agency, which provides their comprehensive assessment of the adequacy and effectiveness of their agency's information security policies, procedures, and practices, must be submitted to OMB. This letter must include the following details, which are specified in 44 USC § 3554:

- **A description of each major incident including**:
  - Threats and threat actors, vulnerabilities, and impacts;
  - Risk assessments conducted on the system before the incident;
  - The status of compliance of the affected information system with security requirements at the time of the incident; and
  - The detection, response, and remediation actions the agency has completed.

- **For each major incident that involved a breach of PII, the description must also include:**
  - The number of individuals whose information was affected by the major incident; and
  - A description of the information that was breached or exposed.

- **The total number of cyber incidents, including a description of system impact levels, types of incident, and locations of affected systems.**

Specifically, in addition to the requirements in 44 USC § 3554, this letter must include the following information:

- **Progress towards meeting FY 2015 FISMA Metrics -** Agency-specific metrics data, as reported through CyberScope, demonstrating agency progress toward meeting the FY 2015 FISMA metrics established by OMB, DHS, and the CIO Council.

- **Progress toward meeting the Cybersecurity CAP goal -** Agencies shall review their performance with regard to the Administration's cybersecurity priorities with their Performance Improvement Officer. Agencies shall include in their annual report information pertaining to the agency's performance in this area.

Agencies shall upload this letter to CyberScope as part of their annual reporting requirements.

FY 2016 FISMA Reporting Timelines

Quarterly Reporting:	CFO Act agencies are required to update administration priority questions (marked "CAP" in the FY 2016 FISMA metrics document) and their supporting metrics (marked "Base" in the FY 2016 FISMA metrics document), at a minimum on a quarterly basis in accordance with the schedule below. Small agencies are encouraged but not required to report on these questions and metrics quarterly. • Quarter 1: no later than January 15, 2016 • Quarter 2: no later than April 15, 2016 • Quarter 3: no later than July 15, 2016 • Quarter 4 / FY 2016 Annual: TBD Agency Inspectors General and Senior Agency Officials for Privacy's information is not required in the quarterly reporting updates, but must be provided for the FY 2016 Annual Report.

Requirement for Explanatory Language in CyberScope

Moving forward, agencies will be required to provide explanatory language within CyberScope for any FISMA metric that does not meet established CAP Goal targets. While there is no minimum length requirement for each comment, agencies are encouraged to provide as much information as needed to best explain their program and progress. This information will be used in conversations between OMB and agency leadership with regard to agencies' cyber programs. Agencies may also provide planned activities for any of the FISMA metrics where new best practices may be beneficial government-wide.

FY 2015-2016 Privacy Management Requirements

As in previous years, the Senior Agency Officials for Privacy are required to report on an annual basis and must submit the following documents through CyberScope as part of the annual data submission:

- Description of the agency's privacy training for employees and contractors;
- Copy of the agency's breach notification policy;
- Progress update on reducing the holdings of personally identifiable information (PII), including eliminating unnecessary use of Social Security numbers; and
- A memorandum describing the agency's privacy program, including:
    - A description of the structure of the agency's privacy program, including the role of the Senior Agency Official for Privacy and the resources that the agency has dedicated to privacy-related functions;[2]

[2] For the purposes of this memorandum, privacy-related functions include, but are not limited to, complying with all laws, regulations, and policies relating to privacy, as well as applying appropriate privacy standards and other best practices.

- An assessment of whether the Senior Agency Official for Privacy has the necessary authority, independence, access to agency leadership, subject matter expertise, and resources to effectively manage and oversee all privacy-related functions across the agency; and
- Any other information OMB should know about how privacy-related functions are performed at the agency.

Agencies are required to submit these documents whether or not the documents have changed from versions submitted in previous years.

Definition of Major Incident

FISMA 2014 requires OMB to define a major incident and directs agencies to report incidents designated as "major" to Congress within seven (7) days. This reporting should follow a process that takes into account the sensitivity of breach details and the classification level of the notification. As such, OMB provides agencies with the following definition and framework for assessing whether an incident is "major".[3]

In determining whether a *Major Incident* has occurred, agencies shall consider whether the incident:

1) Involves information that is Classified, Controlled Unclassified Information (CUI)[4] proprietary, CUI Privacy, or CUI Other;
2) Is not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources; and
3) Has a high or medium functional impact to the mission of an agency; Or
4) Involves the exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems within certain parameters to include either:
   a) A specific threshold of number of records or users affected;[5] or
   b) Any record of special importance.[6]

A *Major Incident* will be characterized by a combination of factors within each table except where noted.

Factor	Definition
Classified	The confidentiality of classified information was compromised

[3] This definition is subject to change based upon incidents, risks, recovery activities, or other relevant factors, and will be updated on MAX.gov https://community.max.gov/x/eQPENw.
[4] http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
[5] 10,000 or more records or 10,000 or more users affected
[6] Any record that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in a significant or demonstrable impact onto agency mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. A collection of records of special importance in the aggregate could be considered an agency High Value Asset.

CUI Proprietary	The confidentiality of controlled unclassified proprietary information, such as protected critical infrastructure information (PCII), controlled intellectual property, or trade secrets was compromised
CUI Privacy	The confidentiality of personal information, or, in some cases, "personally identifiable information," as defined in OMB M-07-16, or "means of identification" as defined in 18 USC 1028(d)(7)
CUI Other	Includes all other categories of CUI not listed above

AND

Factor	**Definition**
Not Recoverable	Recovery from the incident is **not possible** (e.g., sensitive data exfiltrated and posted publicly) (If information was exfiltrated, changed, deleted or otherwise compromised then incident is considered major if either 10,000 or more records or record of special importance was affected)
Not Recoverable within Specified Amount of Time	Time to recover is **unpredictable;** additional resources and outside assistance are needed (10,000 or more users affected)
Recoverable with Supplemental Resources	Time to recover **is predictable** with additional resources (If recovery takes 8 hours or more and 10,000 or more records or record of special importance are affected, then incident should be considered major)

AND

Factor	**Definition**
High Functional Impact	Organization has lost the ability to provide **all** critical services to **all** system users.
Medium Functional Impact	Organization has lost the ability to provide **a** critical service to a **subset** of system users.

OR

Factor	**Definition**
Exfiltration	To obtain, without authorization or in excess of authorized access, information from a system without modifying or deleting it
Modification	The act or process of changing components of information and/or systems
Deletion	To remove information from a system
Unauthorized Access	Logical or physical access without permission to a Federal agency information, system, application, or other resource

Lack of availability	When information, systems, application or services are not accessible or operational

Additional Guidance and Processes for Reporting Major Incidents and Breaches:

- Although agencies may consult with the DHS United States Computer Emergency Readiness Team (US-CERT) on whether an incident is considered a "major incident", it is ultimately the responsibility of the victim agency to make this determination. OMB reserves the right to modify the definition of *Major Incident* based upon incidents, risks, recovery activities, or other relevant factors.

- After the initial agency notification DHS is required to notify OMB within one (1) hour of the relevant agency notifying DHS that a major incident has occurred.

- Agencies shall also notify Congress within 7 days of the date on which the agency has a reasonable basis to conclude that a major incident has occurred; the agency should also notify affected individuals, in accordance with FISMA 2014, as "expeditiously as practicable, without unreasonable delay."

    - After the initial notification to Congress of a major incident, the agency must provide to Congress additional information on the threats, actors, risks, previous risk assessments of the affected system, the current status of the affected system, and the detection, response, and remediation actions that were taken as soon as this information is available.

Section II: Improved Cybersecurity Preparedness and Coordination

This section provides agencies with guidance regarding incident response coordination activities based upon the lessons learned from incidents impacting the Federal government in FY 2015. This section updates procedures to ensure greater consistency in agency response practices, by:

1) Requiring that agencies formally address the need for sensitive positions;
2) Formalizing the process by which agencies can request and receive on-site, technical assistance from DHS;
3) Providing agencies with best practices based upon lessons learned from major cybersecurity incidents

Enhancing Awareness of Cybersecurity Threat Activity

To ensure that agencies can respond to emerging malicious-actor TTPs, all agencies must ensure that, at a minimum, the CIO and the Chief Information Security Officer (CISO) positions are designated as sensitive positions and the incumbents have Top Secret Sensitive Compartmented Information access. This information is necessary given that information regarding malicious-actor TTPs is often classified.

Formalized Process for Providing On-Site, Technical Assistance to Federal Civilian Agencies

Recent cybersecurity events have demonstrated that Federal civilian agencies need a mechanism for quickly responding to incidents, which can include obtaining on-site, technical assistance with the authorization to access relevant agency networks.

Therefore, OMB directs agencies, consistent with applicable law, to provide the following to DHS by emailing rta@us-cert.gov **by November 13, 2015**:

- A standing Federal Network Authorization.[7] Ensure that such an authorization is reviewed on a semiannual basis and remains on file with DHS and will be activated by an email from the victim agency to DHS at the time of an incident;
- A technical point of contact, to be updated as necessary, to facilitate DHS scanning and protective activities within the scope of this memorandum;

Updated Reporting Requirements to Improve Agency Cybersecurity Preparedness

In addition to the establishment of the process for on-site technical assistance, incident response coordination would be improved by clearer points of contact and identification and reporting of HVAs. Agencies will improve coordination with DHS, by:

[7] https://community.max.gov/x/eQPENw

- Designating a principal Security Operations Center (SOC) and reporting this to DHS US-CERT by emailing soc@us-cert.gov by **November 13, 2015**. The principal SOC will be accountable for all incident response activities for that agency.
- Begin reporting their high value assets as first identified in the Cybersecurity Sprint to DHS for ongoing assessment. Identification details and reporting specifics can be found in the HVA guidance which is being provided to agencies on the OMB MAX portal due to its' sensitivity.[8]
- Continuing to provide all public facing IP addresses to the DHS National Cybersecurity Assessment and Technical Services (NCATS) team at ncats@hq.dhs.gov for scanning as directed in OMB M-15-01.

Incident Response Best Practices

These best practices will be provided to Federal agencies through the OMB MAX portal and can be accessed via: https://community.max.gov/x/eQPENw. This information is intended to improve agency plans and procedures that are currently in place, ensure that relevant authorities are documented and understood, and ensure that inter-agency communication is effective so that incidents are mitigated appropriately and as quickly as possible. These best practices are not intended to provide guidance on all incident response activities but focuses on the coordination and communication that is required to effectively respond to and recover from an incident. A successful response effort must align with the policies, procedures, and practices of the agency cyber program, which should support all five functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover).

Points of Contact

Questions for OMB may be directed to ombcyber@omb.eop.gov for security or privacy-oira@omb.eop.gov for privacy. Questions regarding FISMA metrics and CyberScope reporting may be directed to the DHS Federal Network Resilience Division at FNR.FISMA@hq.dhs.gov.

[8] https://community.max.gov/display/Egov/High+Value+Asset+Reporting+Guidance