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

THE DIRECTOR

November 4, 2016

M-17-05

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

SUBJECT: Fiscal Year 2016 – 2017 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) 2016-2017 Federal Information Security Modernization Act (FISMA) and Privacy Management reporting guidance and deadlines, as required by the *Federal Information Security Modernization Act of 2014* (Pub. L. No. 113-283, 128 Stat. 3073) (FISMA 2014), to ensure consistent government-wide performance and best practices to protect national security, privacy and civil liberties while limiting economic and mission impact of incidents.

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 that have the potential to affect the integrity, confidentiality, and/or availability of government information, systems, and services. These incidents demonstrate the need to ensure that we comprehensively address information security practices, policies, and governance. In response to these persistent threats, the Federal Government has taken a number of significant actions to improve Federal information security.

Earlier this year, the President directed his Administration to implement the *Cybersecurity National Action Plan (CNAP)* to increase the level of cybersecurity in both the Federal Government and the larger digital ecosystem. The CNAP builds on the initiatives set forth in *OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*. Concurrent with the release of the CNAP, President Obama

issued an Executive Order establishing the Federal Privacy Council.[1] Furthermore, in July 2016, the Office of Management and Budget (OMB) issued the first update since 2000 to *Circular A-130, Managing Information as a Strategic Resource*, the Federal Government's governing document for the management of Federal information resources. A-130 provides the foundation for the planning, budgeting, governance, acquisition, security, privacy, and management of Federal information resources and codifies a number of important best practices in these areas.

Summary of Contents

Section I: Information Security and Privacy Program Oversight and Reporting Requirements
This section is comprised of requirements to assist agencies with the adoption of Administration priorities and provide OMB the performance indicators necessary to conduct oversight and understand risk through an enterprise-wide lens. Furthermore, this section refines existing guidance to agencies on addressing requirements established in FISMA 2014. Specifically, this section:

- Provides Federal agencies with timelines and requirements for quarterly and annual reporting; and
- Establishes detailed instructions for preparing the annual agency FISMA reports, which must be submitted through the Department of Homeland Security's (DHS) CyberScope reporting system **no later than November 10, 2016**.

Section II: Updated Major Incident Definition and DHS US-CERT Incident Notification Guidelines
This section includes updates to both the definition of "major incident" and the DHS United States Computer Emergency Readiness Team (US-CERT) Incident Notification Guidelines.

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/ewJhRQ

[1] Executive Order 13719, Establishment of the Federal Privacy Council (February 9, 2016)
https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council

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

The following section provides agencies with quarterly and annual FISMA metrics reporting guidelines that serve two primary functions: 1) to ensure agencies are implementing Administration priorities and cybersecurity best practices, and 2) to provide OMB with the data necessary to perform relevant oversight and address risks through an enterprise-wide lens. The existing data collection process continues to inform policy, allows for the performance of targeted oversight, and directs the prioritization of cybersecurity and privacy activities. Agencies will continue to move toward automated data collection and the adoption of a Federal Continuous Diagnostics and Mitigation (CDM) Dashboard, which will begin replacing the current data collection process.

In FY 2016, the FISMA metrics were aligned to the five functions outlined in the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover. The NIST Cybersecurity Framework is a risk-based approach to managing cybersecurity, which is recognized by both government and industry and provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise. Additionally, OMB worked with DHS, the Federal Chief Information Officer (CIO) Council, and the Council of Inspectors General on Integrity and Efficiency to ensure both the CIO metrics and Inspectors General metrics align with the Cybersecurity Framework and provide complementary assessments of the effectiveness of agencies' information security programs.

Federal agencies are to report all of their cybersecurity performance information through DHS's CyberScope reporting system. Agencies shall adhere to the following reporting requirements and timelines:

FY 2016 Annual FISMA Reporting Deadline

Annual FISMA Report:	All Federal agencies, including small and independent agencies, shall report on their performance against the Annual FY 2016 FISMA CIO, Inspector General, and Senior Agency Official for Privacy (SAOP) metrics **by November 10, 2016.**

FY 2016 Agency Reports to OMB and Congress

In accordance with FISMA 2014 (44 U.S.C. § 3554), agencies shall submit an annual report to OMB and DHS; the Committees on Oversight and Government Reform, Homeland Security, and Science, Space, and Technology of the House of Representatives; the Committees on Homeland Security and Government Affairs; and Commerce, Science, and Transportation of the Senate; the appropriate authorization and appropriations committees of Congress; and the Comptroller General.

While agencies must submit their data to OMB by November 10, 2016, agency reports are due to Congress **by March 1, 2017**. OMB does not review or clear these reports, and agencies should

not wait for any such clearance process. Instead, agencies should submit their reports to Congress once they are complete.

Agency Letter – In addition to the aforementioned metrics, agencies must submit a signed letter, marked Controlled Unclassified Information (CUI) if there are specific incident details, from the head of the agency. This letter should provide a comprehensive overview reflecting the agency head's assessment of the adequacy and effectiveness of his or her agency's information security policies, procedures, practices, and include the following details regarding incidents (44 U.S.C. § 3554):

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

- **For each major incident that involved a breach of personally identifiable information (PII),[2] 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 compromised.

- **The total number of incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incidents, and locations of affected information systems.[3]**

In addition to what is specified in 44 U.S.C. § 3554, agencies shall include information regarding incidents reported to US-CERT through the DHS US-CERT Incident Reporting System. Specifically, agencies should:

- Document the number of incidents reported to DHS US-CERT within the FY; and
- Explain any major trends continuing from previous years.

Finally, the letter must include the agency's progress toward meeting FY 2017 FISMA metrics, to include the Cybersecurity Cross Agency Priority (CAP) Goal metrics established by OMB, DHS, and the CIO Council.

---

[2] Per A-130, 'personally identifiable information' refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

[3] "Incident" means an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. 44 U.S.C. § 3552.

Agencies shall upload this letter to CyberScope as part of their annual reporting requirements. Agencies must submit this letter in order to complete their annual reporting package to OMB and may have their cover letters rejected if they fail to provide the required information.

FY 2016 - 2017 Privacy Management Requirements

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

- A description of the agency's compliance with the requirements in A-130 regarding privacy training for employees and contractors;
- A progress update on the agency's reduction of unnecessary holdings of PII, including the elimination of unnecessary uses of Social Security numbers;
- The agency's written policy or procedure for ensuring that any new collection or use of Social Security numbers is necessary;
- A description of the agency's efforts to comply with the privacy-related requirements in OMB M-16-04,[4] including:
    - The number of agency information systems containing PII that have been identified by the agency as High Value Assets (HVAs);
    - For all information systems containing PII that have been identified as HVAs, whether the SAOP has reviewed each information system to determine whether it requires new or updated system of records notices (SORNs) and/or privacy impact assessments (PIAs);
    - Whether all HVAs containing PII that require SORNs and/or PIAs are covered by complete, up-to-date SORNs and/or PIAs; and
    - The number of SORNs and/or PIAs that were published or revised pursuant to the SAOP's review of HVAs;
- 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 SAOP, the placement of the privacy program, and the resources the agency has dedicated to privacy-related functions;[5]
    - A discussion of changes made to the agency's privacy program during the reporting period, including changes in leadership, staffing, structure, and organization, as well as any plans or strategies to make changes in the future;
    - Links to relevant publicly available documents and materials, including the policies, procedures, structure, roles, and responsibilities with respect to the agency's privacy program and the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII; and

[4] CSIP required agencies to identify HVAs that contain PII; recommend whether particular systems should be added to the agency's list of HVAs; and review all HVAs containing PII to ensure that any SORNs and PIAs are current, accurately address risks to PII, and include any steps taken to mitigate those risks. *See* OMB Memorandum M-16-04.

[5] 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.

- Any other information that OMB should know regarding privacy-related functions performed at the agency.

Moving Forward: FY 2017 FISMA Reporting Timelines

Quarterly Reporting:	Chief Financial Officer (CFO) Act agencies[6] are required to update their responses to FISMA questions and metrics, at a minimum, on a quarterly basis in accordance with the schedule below. Questions and metrics marked "CAP" in the FISMA guidance will be used in recurring OMB publications such as the quarterly Cybersecurity CAP Goal Report published on Performance.gov. All agencies should update all FISMA questions and metrics as often as needed (i.e., more often than each quarter) to ensure agency leadership has useful, up-to-date information. Small agencies are encouraged, but not required, to report on these questions and metrics each quarter. Agencies should provide explanatory language in the optional comment field within CyberScope for any FISMA metric that does not meet established CAP goal targets or for which significant progress or impediments warrant OMB's attention or assistance. All agencies that are participants in the President's Management Council (PMC) Cybersecurity Assessment Process must report their quarterly PMC Cybersecurity Self Assessments in accordance with the schedule below. • Quarter 1: no later than January 15, 2017 • Quarter 2: no later than April 15, 2017 • Quarter 3: no later than July 15, 2017 • Quarter 4 / FY 2017 Annual: no later than October 31, 2017 Agency Inspectors General and SAOPs information is not required quarterly, but must be provided for the FY 2017 Annual Report to Congress. Although the information provided by the SAOPs is only required to be submitted to OMB on an annual basis, all agencies should update all FISMA questions and metrics as often as needed to ensure agency leadership has useful, up-to-date information.

[6] 31 U.S.C. § 901 (b), as amended.

Section II: Updated Major Incident Definition and DHS US-CERT Incident Notification Guidelines

Updated Definition of Major Incident

FISMA 2014 authorizes OMB to define the term "major incident" and further directs agencies to notify Congress of a "major incident." This Memorandum provides agencies with a definition and framework for assessing whether an incident[7] is a "major incident" for purposes of the Congressional reporting requirements under FISMA 2014.[8] This Memorandum also provides specific considerations for determining when a breach[9] constitutes a "major incident." This guidance replaces the "major incident" definition previously provided in OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirement*.

A "major incident" is any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.[10] Agencies should determine the level of impact of the incident by using the existing incident management process established in NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide, and are encouraged to use the US-CERT National Cybersecurity Incident Scoring System (NCISS), which uses the following factors:[11]

- Functional Impact;
- Observed Activity;
- Location of Observed Activity;
- Actor Characterization;
- Information Impact;
- Recoverability;
- Cross-Sector Dependency; and
- Potential Impact.

---

[7] An "incident" is defined under FISMA 2014 as "an occurrence that – (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." 44 U.S.C. § 3552(b)(2).

[8] *See* 44 U.S.C. § 3554(b)(7).

[9] A breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses PII for an other than authorized purpose. The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.

[10] Level 3 (orange) or higher on the Cyber Incident Severity Schema, which includes a Level 4 event (red) defined as one that is "likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties," and a Level 5 event (black), defined as one that "poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons."

[11] https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

Appropriate analysis of the incident will include the agency CIO, the Chief Information Security Officer (CISO), mission or system owners, and if the occurrence is a breach, the SAOP. The definition above leverages the NCISS and therefore creates uniformity in terminology and criteria utilized by agencies and the US-CERT incident responders.

Other than breaches (which are addressed separately), if the incident meets the definition of a "major incident," it is also a "significant cyber incident" for purposes of PPD-41.[12] Thus, a "major incident" as defined above will also trigger the coordination mechanisms outlined in PPD-41, including a Cyber Unified Coordination Group (CUCG).

A Breach that Constitutes a Major Incident

A breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.[13] An unauthorized modification of,[14] unauthorized deletion of,[15] unauthorized exfiltration of,[16] or unauthorized access to[17] 100,000 or more individuals' PII constitutes a "major incident."[18]

Congressional Reporting

Agencies must notify appropriate Congressional Committees per FISMA 2014[19], of a "major incident" no later than seven (7) days after the date on which the agency determined that it has a reasonable basis to conclude that a "major incident" has occurred.[20] This report should take into account the information known at the time of the report, the sensitivity of the details associated with the incident, and the classification level of the information. When a "major incident" has occurred, the agency must also supplement its initial seven (7) day notification to Congress with

---

[12] https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[13] The analysis for reporting a major breach to Congress is distinct and separate from the assessment of the potential risk of harm to individuals resulting from a suspected or confirmed breach. When assessing the potential risk of harm to individuals, agencies should refer to OMB's guidance on preparing for and responding to a breach of PII.

[14] Unauthorized modification is defined as the act or process of changing components of information and/or information systems.

[15] Unauthorized deletion is defined as the act or process of removing information from an information system.

[16] Unauthorized exfiltration is defined as the act or process of obtaining, without authorization or in excess of authorized access, information from an information system without modifying or deleting it.

[17] Unauthorized access is defined as the act or process of logical or physical access without permission to a Federal agency information, information system, application, or other resource.

[18] Only when a breach of PII that constitutes a "major incident" is the result of a cyber incident will it meet the definition of a "significant cyber incident" and trigger the coordination mechanisms outlined in PPD-41

[19] The Committee on Oversight and Government Reform, Committee on Homeland Security, and the Committee on Science, Space, and Technology of the House of Representatives; the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate; and the appropriate authorization and appropriations committees of Congress. *See* 44 U.S.C. § 3554(b)(7)(C)(iii)(III).

[20] Thus, once an agency (based on initial incident analysis) arrives at a reasonable basis to conclude that a major incident has occurred, it must then report the suspected major incident to Congress within seven (7) days.

pertinent updates within a reasonable period of time after additional information relating to the incident is discovered. This supplemental report must include summaries of:

- The threats and threat actors, vulnerabilities, and impacts relating to the incident;
- The risk assessments conducted of the affected information systems before the date on which the incident occurred;
- The status of compliance of the affected information systems with applicable security requirements at the time of the incident; and
- The detection, response, and remediation actions.

Congressional Reporting of a Breach

Agencies must notify appropriate Congressional Committees per FISMA 2014[21] no later than seven (7) days after the date on which there is a reasonable basis to conclude that a breach that constitutes a "major incident" has occurred. In addition, agencies must also supplement their initial seven (7) day notification to Congress with a report no later than 30 days after the agency discovers the breach.[22] This supplemental report must include:[23]

- A summary of information available about the breach, including how the breach occurred, based on information available to agency officials on the date which the agency submits the report;
- An estimate of the number of individuals affected by the breach, including an assessment of the risk of harm to affected individuals, based on information available to agency officials on the date on which the agency submits the report;
- A description of any circumstances necessitating a delay in providing notice to affected individuals; and
- An estimate of whether and when the agency will provide notice to affected individuals.

Nothing in this guidance is intended to preclude an agency reporting an incident or a breach to Congress that does not meet the threshold for a major incident.

Additional Guidance and Processes for Reporting Major Incidents:

- Although agencies may consult with DHS US-CERT on whether an incident is considered a "major incident," it is ultimately the responsibility of the impacted agency to make this determination.

[21] The Committee on Oversight and Government Reform, Committee on Homeland Security, and the Committee on Science, Space, and Technology, of the House of Representatives; the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate; the appropriate authorization and appropriations committees of Congress; the Committee on the Judiciary of the Senate; and the Committee on the Judiciary of the House of Representatives. *See* 44 U.S.C. § 3553, note ("Breaches").
[22] 44 U.S.C. § 3553, note ("Breaches").
[23] *Id.*

- Agencies should report to DHS US-CERT within one (1) hour of determining an incident to be "major," or should update US-CERT within one (1) hour of determining that an already-reported incident has been determined to be major.

- If the agency determines a major incident has occurred, DHS is then required to notify OMB within one (1) hour of being so alerted.

Updated Reporting Requirements for Agencies and US-CERT

OMB and DHS are instituting processes, described below, to improve Federal incident data to better understand information security incident trends, determine the impact incidents have on Federal agencies, and inform government-wide policies to improve information security protections.

In October 2016, US-CERT released updated incident reporting guidelines to agencies that specify additional mandatory reporting fields for the US-CERT Incident Reporting System. To assist agencies in using the new guidelines, DHS will host a series of information sessions to familiarize agencies with the updated reporting fields and agencies will begin reporting in this revised format by April 1, 2017.

Agencies and US-CERT will also now participate in a formal data validation process to ensure the reported incident data is comprehensive and accurate. This improved information will serve as a foundation for agencies and DHS to perform investigative and forensic work. The framework for this process is as follows:

- US-CERT will provide every Federal agency with a log of the incidents it has reported by the 5th day of each quarter; and
- Agencies will review and validate that the data is correct and up to date by the 20th day of each quarter.

OMB will provide a high-level summary of agency incident data in the Annual FISMA Report to Congress in accordance with 44 U.S.C. § 3553.

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.

APPENDIX A: FY 2016-2017 REQUIREMENTS TRACKER

This Appendix documents specific action items including deadlines and action item owners. Engagement will occur as needed to close out the action items

Number	Action	Deadline	Responsible Party
#1	Report agency performance against the Annual FY 2016 FISMA CIO, Inspector General, and Senior Agency Official for Privacy metrics.	November 10, 2016	All agencies
#2	Privacy Program Memorandum.	November 10, 2016	All agencies
#3	Deliver agency annual report, including agency head letter, to Congress.	March 1, 2017	All agencies
#4	Update responses to FISMA questions and metrics at least quarterly.	Quarter 1: no later than January 15, 2017 Quarter 2: no later than April 15, 2017 Quarter 3: no later than July 15, 2017 Quarter 4 / FY 2017 Annual: no later than October 31, 2017	CFO Act agencies
#5	Report incidents designated as "major" to Congress within seven (7) days of the date on which the agency has a reasonable basis to conclude a major incident has occurred.	Ongoing	All agencies
#6	Notify OMB within one (1) hour of an agency notifying DHS that a major incident has occurred.	Ongoing	DHS
#7	Notify affected individuals, in accordance with FISMA 2014, as "expeditiously as practicable, without unreasonable delay."	Ongoing	All Agencies
#8	Following the identification of an incident as "major," provide to Congress, as soon as it is available, additional information on the threats, actors, and risks posed, as well as previous risk assessments of the affected	Ongoing	All Agencies

	system, the current status of the affected system, and the detection, response, and remediation actions that were taken.		
#9	Reporting in the revised US-CERT Incident Reporting System format.	April 1, 2017	All Agencies
#10	US-CERT will provide every Federal agency with a log of information security incidents it has reported over the previous quarter.	5th day of each quarter	DHS
#11	Agencies will validate that the data provided by US-CERT is correct and up to date.	20th day of each quarter	All Agencies