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

THE DIRECTOR

October 16, 2017

M-18-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Mick Mulvaney
Director

SUBJECT: Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements

Purpose

This memorandum provides agencies with Fiscal Year (FY) 2017-2018 Federal Information Security Modernization Act of 2014 (FISMA) reporting guidance and deadlines.[1] FISMA requires the Office of Management and Budget (OMB) to oversee agency information security policies and practices. [2] This memorandum describes the processes for Federal agencies[3] to report to OMB and, where applicable, the Department of Homeland Security (DHS). This memorandum does not apply to national security systems or intelligence community systems, although both communities may leverage the document to inform their management processes.

Additionally, this memorandum consolidates requirements from prior OMB annual FISMA guidance to ensure consistent, government-wide performance and agency adoption of best practices. This consolidation also addresses the burden reduction requirements in OMB Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memorandum*. Accordingly, OMB rescinds the following memoranda:

- OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*;
- OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*; and
- OMB Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*.

Section I of this memorandum describes Information Security Program Oversight and FISMA Reporting Requirements and includes deadlines for all Federal agencies' quarterly and annual FISMA metrics. These reporting requirements also fulfill the requirement for agencies to conduct regular risk management assessments established in Executive Order (EO) 13800 "Strengthening

[1] 44 U.S.C. § 3551 et. seq.
[2] 44 U.S.C. § 3553
[3] 44 U.S.C. § 3502

the Cybersecurity of Federal Networks and Critical Infrastructure." Section II describes continuing Incident Reporting Guidelines, including the requirements maintained from the rescinded M-15-01, M-16-03, and M-17-05.

Section I: Information Security Program Oversight and FISMA Reporting Requirements

I. Reporting to OMB and DHS

FISMA requires agencies to report on the status of their information security programs to OMB. Each year, OMB and DHS work with an interagency working group to develop Chief Information Officer (CIO) FISMA metrics to track agencies' progress implementing cybersecurity capabilities. OMB and DHS also collaborate with the Inspectors General (IG) community to ensure that the IG FISMA metrics provide independent assessments of agency information security programs in accordance with FISMA requirements.

During FY 2017, OMB and DHS leveraged the CIO and IG FISMA metrics to assess federal civilian agencies' risk management to comply with EO 13800. OMB will use the FY 2018 FISMA reporting process to conduct these risk management assessments for FY 2018. At a minimum, CFO Act agencies must update their data quarterly and non-CFO Act agencies must update their data on a semiannual basis. Table I provides the quarterly and annual reporting deadlines for FY2017 and FY2018.

Table I: Annual and Quarterly FISMA Reporting Deadlines

Reporting Period	Deadline	Responsible Parties
FY 2017 Annual CIO, IG, and Senior Agency for Privacy (SAOP) FISMA Reporting	October 31, 2017	All Civilian Agencies
FY 2018 Q1 CIO FISMA Reporting	January 15, 2018	CFO Act Agencies
FY 2018 Q2 CIO FISMA Reporting	April 16 2018	All Civilian Agencies
FY 2018 Q3 CIO FISMA Reporting	July 16, 2018	CFO Act Agencies
FY 2018 Annual CIO, IG, and SAOP FISMA Reporting	October 31, 2018	All Civilian Agencies

The metrics represent baseline security controls that all agencies must meet. OMB and DHS use these metrics in the ongoing Risk Management Assessment process pursuant to EO 13800. Starting in FY2018, all federal civilian agencies must respond to all questions in these metrics submissions. Additionally, agency CIOs and IGs are strongly encouraged to engage in discussions related to agency progress toward addressing the IG FISMA metrics.

II. Agency Head Letter for Annual Reporting Requirement to OMB

In addition to the CIO, IG, and Senior Agency Officials for Privacy (SAOP) FISMA metrics, agencies must also include in the agency's annual reporting package to OMB a signed letter from

the head of the agency to the OMB Director and the Secretary of Homeland Security. The letter must contain the following criteria:[4]

1. A detailed assessment of the adequacy and effectiveness of the agency's information security policies, procedures, and practices, including details on progress toward meeting FY 2017 government-wide targets in the Cybersecurity Cross-Agency Priority Goal metrics.
2. Details on the total number of incidents reported to the DHS United States Computer Emergency Readiness Team (US-CERT) through the DHS US-CERT Incident Reporting System. In the event of a major incident, the agency must provide: a description of each incident, system impact levels, types of incidents, and locations of affected information systems.[5]
3. A description of each major incident, if applicable, with the following details:
    - 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.

Federal civilian agencies must upload this letter to CyberScope as part of their annual reporting requirements and may have their cover letters rejected if they fail to provide the required information.

As in previous years, SAOPs are required to report annually and must submit each of the following items as separate documents through CyberScope:

- The agency's privacy program plan;[6]
- A description of any changes made to the agency's privacy program during the reporting period, including changes in leadership, staffing, structure, and organization;
- The agency's breach response plan;[7]

[4] 44 U.S.C. § 3554.

[5] FISMA defines "incident" 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).

[6] Each agency is required to develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program. See OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 4(c)(2), 4(e)(1) (July 28, 2016). Additionally, reporting by entities other than federal Executive Branch civilian agencies is voluntary.

[7] Each agency is required to develop and implement a breach response plan. A breach response plan is a formal document that includes the agency's policies and procedures for reporting, investigating, and managing a breach. It should be specifically tailored to the agency and address the agency's missions, size, structure, and functions. *See*

- The agency's privacy continuous monitoring strategy;[8]
- The Uniform Resource Locator (URL) for the agency's privacy program page,[9] as well as the URL for any other sub-agency-, component-, or program-specific privacy program pages; and,
- The agency's written policy or procedure to ensure that any new collection or use of Social Security numbers (SSNs) is necessary, along with a description of any steps the agency took during the reporting period to explore alternatives to the use of SSNs as a personal identifier.[10]

III. Annual Reporting to Congress and the Government Accountability Office

In addition to requiring the submission of agency annual FISMA reports to OMB and DHS, FISMA requires agencies to submit their annual FISMA reports to the Chairperson and Ranking Member of the following Congressional committees:[11]

1. House Committee on Oversight and Government Reform;
2. House Committee on Homeland Security;
3. House Committee on Science, Space, and Technology;
4. Senate Committee on Homeland Security and Government Affairs;
5. Senate Committee on Commerce, Science, and Transportation; and
6. The appropriate authorization and appropriations committees of the House and Senate.

Additionally, agencies must provide a copy of their reports to the Comptroller General of the United States.

Agency reports are due to Congress and the Government Accountability Office (GAO) **by March 1, 2018**.[12]

OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017).

[8] Each agency is required to develop and maintain a privacy continuous monitoring strategy. A privacy continuous monitoring strategy is a formal document that catalogs the available privacy controls implemented at an agency across the agency risk management tiers and ensures that the controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. *See* OMB Circular A-130, Information as a Strategic Resource (July 28, 2016).

[9] Each agency is required to maintain a central resource page dedicated to its privacy program on the agency's principal website. The agency's Privacy Program Page must serve as a central source for information about the agency's practices with respect to PII. The agency's Privacy Program Page must be located at www.[agency].gov/privacy and must be accessible through the agency's "About" page. *See* OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services (November 8, 2016).

[10] Each agency is required to take steps to eliminate unnecessary collection, maintenance, and use of Social security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier. See OMB Circular A-130, Information as a Strategic Resource (July 28, 2016).

[11] 44 U.S.C. § 3554.

[12] OMB <u>will not</u> review, clear, or provide a template for the reports. Agencies should submit the reports directly to Congress and the GAO.

Section II: Incident Reporting Guidelines

The following guidance is intended to assist agencies in submitting incident response data and coordinating with the responsible authorities.

Major Incident Definition

FISMA directs OMB to define the term "major incident" and further instructs agencies to notify Congress in the event of a "major incident." This memorandum provides agencies with a definition and framework for assessing whether an incident is a major incident for purposes of the Congressional reporting requirements under FISMA. This memorandum also provides specific considerations for determining the circumstances under which a breach constitutes a major incident.

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.[13] Agencies should determine the level of impact of the incident by using the existing incident management process established in National Institute of Standards and Technology (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:[14]

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

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

A breach is a type of incident and constitutes a major incident when it involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is

[13] 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."
[14] https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

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.[15] While agencies should assess each breach on a case-by-case basis to determine whether it meets the definition of a major incident, an unauthorized modification of,[16] unauthorized deletion of,[17] unauthorized exfiltration of,[18] or unauthorized access to[19] 100,000 or more individuals' PII automatically constitutes a major incident.[20] Breach reporting requirements are outlined in OMB M-17-12.

Pursuant to Presidential Policy Directive-41 (PPD-41), if an incident is a major incident, it is also a "significant cyber incident". Thus, a major incident as defined above will also trigger the coordination mechanisms outlined in PPD-41 and potentially require participation and actions from a Cyber Unified Coordination Group.

An agency must notify the appropriate Congressional Committees and its OIG of a major incident no later than seven days after the date on which the agency determined that it has a reasonable basis to conclude that a major incident has occurred. [21] 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 day notification to Congress with 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.

[15] 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 M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.

[16] "Unauthorized modification" is the act or process of changing components of information and/or information systems without authorization or in excess of authorized access.

[17] "Unauthorized deletion" is the act or process of removing information from an information system without authorization or in excess of authorized access.

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

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

[20] 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

[21] FISMA requires notification to the House of Representatives Committees on: (1) Oversight and Government Reform; (2) Homeland Security; and (3) Science, Space, and Technology; and to the Senate Committees on: (1) Homeland Security and Governmental Affairs and (2) Commerce, Science, and Transportation; as well as to the appropriate authorization and appropriations committees. *See* 44 U.S.C. § 3554(b)(7)(C)(iii)(III).

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

- 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 from reporting an incident or breach to Congress that does not meet the threshold for a major incident.

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

- Agencies should report to DHS US-CERT within one hour of determining an incident to be 'major,' or should update US-CERT within one hour of determining that an already-reported incident has been determined to be major.
- If the agency determines that a major incident has occurred, DHS must notify OMB within one hour of being informed of the incident

Reporting a Breach to US-CERT[23]

In coordination with the National Security Council and OMB, DHS shall update the US-CERT Incident Notification Guidelines and associated reporting forms, providing agencies with details and standardized procedures for reporting a breach.

Scanning Internet Accessible Addresses and Systems

OMB directs DHS to take the following actions in the interest of improving Federal information security. These responsibilities are subject to OMB oversight and applicable FISMA

[22] FISMA requires notification to the House of Representatives Committees on: (1) Oversight and Government Reform; (2) Homeland Security; (3) Science, Space, and Technology; and (4) the Judiciary; and to the Senate Committees on: (1) Homeland Security and Governmental Affairs; (2) Commerce, Science, and Transportation; and (3) the Judiciary; as well as to the appropriate authorization and appropriations committees. *See* 44 U.S.C. § 3553, note ("Breaches").

[23] OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.

requirements and limitations. In furtherance of those responsibilities and consistent with applicable law, regulation, policy, and existing Memoranda of Agreement with agencies, DHS shall:

- Scan internet accessible addresses and public facing segments of Federal civilian agency systems for vulnerabilities on an ongoing basis as well as in response to newly discovered vulnerabilities.[24]

Each Federal civilian agency shall, consistent with Binding Operational Directive 15-01:

- Ensure that its standing Federal Network Authorization remains on file with DHS for incident response and hunt assistance;
- Ensure that an authorization remains on file with DHS for scanning of internet accessible addresses and systems, and that such authorization is reviewed semiannually ; and,
- Continue to provide DHS a complete list of all internet accessible federal information systems and related addressing information semiannually, including static Internet Protocol (IP) addresses for external websites, servers, and other access points and domain name service names for dynamically provisioned systems.[25] Provide DHS with at least five business days advanced notice of changes to IP ranges by emailing NCATS@hq.dhs.gov.

Facilitating Incident Coordination

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

Agencies will improve coordination with DHS, by:

- Designating a principal Security Operations Center (SOC) and reporting this to DHS US-CERT via email to soc@us-cert.gov. The principal SOC will be accountable for all incident response activities for that agency, to include notifying US-CERT of any PII incidents or security breaches.

Agencies must report incidents to DHS US-CERT according to the current requirements in the US-CERT Federal Incident Notification Guidelines as required by 44 U.S.C. § 3554(b)(7)(C)(ii).

[24] On an emergency basis, and where not prohibited by law, internet accessible addresses and public facing segments of Federal civilian agency systems may be scanned without prior agency authorization.
[25] The term "dynamically provisioned system" refers to systems which are virtually hosted and operated from multiple sites, such that network traffic to the systems is distributed across multiple, discrete IP ranges or autonomous system numbers (ASNs). *See BOD 15-01.*

Points of Contact

Agencies should direct questions on program performance to OMB Cyber at ombcyber@omb.eop.gov.

Agencies should direct privacy-related matters to OMB's Office of Information and Regulatory Affairs (OIRA) at privacy-oira@omb.eop.gov.

Agencies should direct questions on CyberScope reporting to the DHS Federal Network Resilience Division at FNR.FISMA@hq.dhs.gov.

Agencies should direct questions on FISMA metrics to OMB Cyber and DHS Federal Network Resilience Division.

APPENDIX A: FY 2017-2018 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 2017 FISMA CIO, Inspector General, and Senior Agency Official for privacy metrics.	October 31, 2017	All civilian agencies
#2	Provide agency annual report, including agency head letter, to Congress and the GAO.	No later than March 1, 2018	All civilian agencies
#3	Update responses to FISMA questions and metrics at least quarterly.	Quarter 1: no later than January 15, 2018	CFO Act agencies
		Quarter 2: no later than April 16, 2018	All civilian agencies
		Quarter 3: no later than July 15, 2018	CFO Act agencies
		Quarter 4 / FY 2018 Annual: no later than October 31, 2018	All civilian agencies
#4	Following the identification of an incident as "major," agencies shall: • Notify affected individuals expeditiously as practicable, without unreasonable delay • 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 system, the current status of the affected system, and the detection, response, and remediation actions that were taken.	Ongoing	All civilian agencies

#5	Ensure that, at a minimum, the CIO and the CISO positions are designated as sensitive positions and the incumbents have Top Secret Sensitive Compartmented Information access.	Ongoing	All civilian agencies