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

THE DIRECTOR

November 9, 2020

M-21-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements

Purpose

This memorandum provides agencies with fiscal year (FY) 2021 reporting guidance and deadlines in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).[1] This memorandum also consolidates several government-wide reporting requirements to eliminate duplicative or burdensome processes in accordance with the requirements in Office of Management and Budget (OMB) Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*. Accordingly, OMB rescinds the following memoranda:

- M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*

This memorandum does not apply to national security systems,[2] although agencies are encouraged to leverage the document to inform their management processes.

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

I. Reporting to the Office of Management and Budget and the Department of Homeland Security

FISMA requires agencies to report the status of their information security programs to OMB and requires Inspectors General (IG) to conduct annual independent assessments of those programs. OMB and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) collaborate with interagency partners to develop the Chief Information Officer (CIO) FISMA metrics, and with IG partners to develop the IG FISMA metrics to facilitate these processes. OMB also works with the Federal privacy community to develop

[1] 44 U.S.C. § 3551 et. seq.
[2] As defined in 44 U.S.C. § 3552.

Senior Agency Official for Privacy (SAOP) metrics. These three sets of metrics together provide a comprehensive picture of an agency's cybersecurity and privacy performance.

CIO and IG Reporting: OMB and CISA use CIO and IG reporting to compile agency-specific and government-wide risk management assessments as part of an ongoing effort in support of Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*

At a minimum, Chief Financial Officer (CFO) Act[3] agencies must update their CIO Metrics quarterly and non-CFO Act agencies must update their CIO metrics on a semiannual basis. Reflecting the Administration's shift from compliance to risk management, as well as the guidance and requirements outlined in OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, and Binding Operational Directive 18-02, Securing High Value Assets, CIO Metrics are not limited to assessments and capabilities within National Institute of Standards and Technology (NIST) security baselines, and agency responses should reflect actual implementation levels. Although FISMA requires an annual IG assessment, OMB strongly encourages CIOs and IGs to discuss the status of information security programs throughout the year.

SAOP Reporting: Given the importance of privacy, as highlighted in policies such as OMB Circular A-130, *Managing Information as a Strategic Resource*, and OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, agencies must take appropriate measures to comply with privacy requirements and manage privacy risks. 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;[4]
- 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;[5]
- The agency's privacy continuous monitoring strategy;[6]
- The Uniform Resource Locator (URL) for the agency's privacy program page,[7] as well as the URL for any other sub-agency-, component-, and/or program-specific privacy program pages; and,
- The agency's written policy 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.[8]

---

[3] See Chief Financial Officers Act of 1990.
[4] See OMB Circular A-130, Appendix I § 4(c)(2), 4(e)(1).
[5] See OMB M-17-12.
[6] See OMB Circular A-130, Appendix I § 4(d)(9), 4(e)(2).
[7] See OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*.
[8] See OMB Circular A-130, Appendix I § 5(f)(1)(f)

Table I provides the quarterly and annual reporting deadlines for remainder of FY 2020 and FY 2021.

Consistent with adjustments to agency reporting deadlines found in OMB Memorandum M-20-21, *Implementation Guidance for Supplemental Funding Provided in Response to the Coronavirus Disease 2019 (COVID-19)*, the COVID-19 national emergency may disrupt the ability of agencies to meet their reporting requirements in a timely manner. IGs and other independent assessors who are unable to conduct portions of their independent assessments in person are encouraged to conduct assessments remotely to the greatest extent practicable. Agencies that believe they will be unable to meet reporting deadlines should direct requests for extension to OMB at ombcyber@omb.eop.gov (for IG or CIO submissions) or privacy-oira@omb.eop.gov (for SAOP submissions). This request should include a justification and target date of completion.

Table I: Annual and Quarterly FISMA Reporting Deadlines

Reporting Period	Deadline	Responsible Parties
FY 2020 Annual CIO, IG, SAOP FISMA Reporting	November 2, 2020[9]	All Agencies
FY 2021 Q1 CIO FISMA Reporting	January 15, 2021	CFO Act Agencies
FY 2021 Q2 CIO FISMA Reporting	April 15, 2021	All Agencies
FY 2021 Q3 CIO FISMA Reporting	July 15, 2021	CFO Act Agencies
FY 2021 Annual CIO, IG, and SAOP FISMA Reporting	October 29, 2021	All Agencies

II. Agency Head Letter for Annual Reporting Requirement to OMB

FISMA requires that agency heads are ultimately responsible for ensuring that their respective agencies maintain protections commensurate with the risk of harm of a compromise. Agency heads must maintain awareness of their agency's information security programs and direct CIOs and Chief Information Security Officers (CISOs) to implement appropriate security measures and, where necessary, take remedial actions to address known vulnerabilities and threats.

Requirement: In an effort to verify the agency head's awareness and to validate the agency's FISMA report, OMB requires a signed letter from the agency head to the OMB Director and DHS Secretary as part of their annual reporting package to OMB. The letter must contain the following information:[10]

A. 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 2020 government-wide targets in the CIO FISMA metrics;

[9] This date is an update from the instructions provided in M-20-04.
[10] 44 U.S.C. § 3554.

B. Details on the total number of information security incidents reported through the CISA Incident Reporting System;[11] and
C. A description of each major incident, if applicable, with the following details:
    - The incident description to include attack vector, response, and remediation actions the agency has completed;
    - Threats and threat actors, vulnerabilities, and mission and system impacts;
    - Risk assessments conducted on the information system before the date of the major incident; and
    - The status of compliance of the affected information system with security requirements at the time of the major incident.

Reporting Method: Agencies must upload this letter to CyberScope as part of their annual submission. Agencies shall not send OMB or DHS hardcopy submissions.

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:[12]

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, 2021**.[13]

Section II: Incident Reporting Requirements

Incident reporting is vital to understanding government-wide threats and aiding in incident response. Effective incident reporting provides insight on attack vectors, time to detect, and time to restore operations. OMB is providing the following guidance to assist agencies in submitting incident response data and to promote coordination with the responsible authorities.

---

[11] 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).

[12] 44 U.S.C. § 3554.

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

Incident Reporting

Agencies must report incidents to CISA according to the current and updated requirements in the CISA Federal Incident Notification Requirements[14] This includes events that have been under investigation for 72 hours without successful determination of the event's root cause or nature (i.e., malicious, suspicious, benign).

This reporting also includes determining the impact category, attack vector, and incident attributes. CISA then uses these details, as well as several other categories of information, to produce a CISA Cyber Incident Scoring System score, which provides a repeatable and consistent mechanism for estimating the risk of an incident.

In order to ensure OMB is able to maintain appropriate situational awareness and oversight of incidents impacting the Federal enterprise, CISA shall provide OMB with the following:

#	Action	Deadline
1	Incident details on all incidents received through the CISA Incident Reporting System to be delivered on a monthly basis.	No later than the 15th of each month.
2	Summary report of all incidents scored as a medium (yellow) priority-level and above, including whether these were elevated as a result of a campaign and the weights for each category.	No later than the 15th of each month.

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 and provides specific considerations for determining the circumstances under which a breach constitutes a major incident. Additionally, this guidance does not preclude an agency from reporting an incident or breach to Congress that falls below the threshold for a major incident.

A major incident is EITHER:

I. Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.[15] Agencies

[14] 44 U.S.C. §§ 3553(b)(2)(A), FISMA also requires agencies to notify and consult with the Federal information security incident center established in section 3556 of title 44 U.S. Code regarding any information security incidents; 44 U.S.C. § 3554(b)(7)(C)(ii).

[15] Using the CISA Cyber Incident Scoring System, this includes Level 3 events (orange), defined as those that are "likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence"; Level 4 events (red), defined as those that are "likely to result in a

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*,

OR,

II. A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.[16]

While agencies should assess each breach on a case-by-case basis to determine whether the breach meets the definition of a major incident, this memorandum requires a determination of major incident for any unauthorized modification of, [17] unauthorized deletion of,[18] unauthorized exfiltration of,[19] or unauthorized access to[20] the PII of 100,000 or more people. OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* details breach reporting requirements.

Appropriate analysis of the incident will include the agency CIO, CISO, mission or system owners, and, if a breach, the SAOP as well. Agencies may consult with OMB and CISA to make a major incident determination.

Reporting Major Incidents

I. Reporting to OMB and CISA.

- Agencies must report to CISA and the OMB Office of the Federal Chief Information Officer (OFCIO) within one hour of determining a major incident occurred, and should update OMB OFCIO and CISA within one hour of determining that an already-reported incident or breach has been determined to be a major incident.[21]

---

significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties"; and Level 5 events (black), defined as those that "pose an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons."

[16] 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.

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

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

[19] "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.

[20] "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.

[21] This reporting is limited to the time after a major incident determination is made and not just the detection of the incident; it is expected that an agency will take some time to determine if an incident or breach reaches the threshold to be considered "major."

- Pursuant to Presidential Policy Directive-41 (PPD-41), *United States Cyber Incident Coordination*, 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.

II. Reporting to Congress and Inspectors General

- 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, including a breach constituting a major incident, has occurred. [22]
- 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 notification to Congress with pertinent updates within a reasonable period of time after additional information relating to the incident is discovered. The 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.

- In addition, agencies must also supplement their seven day report to Congress with another report no later than 30 days after the agency discovers a breach constituting a major incident.[23] 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 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 the agency submits the report;

---

[22] 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).

[23] 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"); OMB M-17-12 § VII.D.3.

- 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.

Section III: Strengthening Continuous Diagnostics and Mitigation Capabilities

CDM Program Overview

The Continuous Diagnostics and Mitigation (CDM) Program enhances the overall security posture of the Federal Government by providing Federal agencies with capabilities to monitor vulnerabilities and threats to their networks in near real-time. This increased situational awareness allows agencies to prioritize actions to mitigate or accept cybersecurity risks based on an understanding of the potential impacts to their mission. CDM accomplishes this by working with agencies to deploy commercial off-the-shelf tools on agency networks that provide enterprise-wide visibility of what assets, users, and activities are on their networks. This actionable information enables agencies to effectively monitor, defend, and rapidly respond to cyber incidents.

The CISA CDM Program Management Office (PMO) categorizes participating agencies into groups for the purposes of bundling task orders and enabling closer oversight of agencies' CDM implementation. All Chief Financial Officer (CFO) Act agencies, with the exception of the Department of Defense (DOD), participate in CDM along with dozens of non-CFO Act agencies. While the CDM PMO, working with the General Services Administration (GSA), manages related contracts on behalf of the agencies, agencies are solely responsible for the state of their cybersecurity posture and must work closely with CISA in order to accomplish CDM program goals within their respective agencies.

CDM Implementation & Agency Responsibilities and Expectations

Federal Dashboard Deployment and Operations

CISA will maintain a fully operational Federal Dashboard to provide, in aggregate, situational awareness of the Federal Government's overall cybersecurity posture. Federal agencies with the dashboard capabilities in place can exchange data with the Federal Dashboard, provided they have the technical capabilities to operate, maintain, and exchange the data. To assist agencies with meeting these standards, CISA will make available to agencies the CDM Program Data Quality Management Plan (DQMP). The CDM PMO and CFO Act agencies, using the DQMP, will work together to ensure that all CFO Act agencies are **certified** and fully able to exchange timely data to the Federal Dashboard by the end of FY21 Q4. CFO Act agencies unable to meet this target date must provide a written justification to both OMB and CISA.[24] Additionally, the CDM PMO and participating non-CFO Act agencies will work together to ensure that all participating non-CFO Act agencies establish information exchange between their respective dashboards and the Federal Dashboard by the end of the end of FY21 Q4.

[24] This justification should be signed by the agency CIO.

Acquiring Capabilities

CDM currently provides agencies with an efficient and cost-effective approach for achieving Government-wide information security continuous monitoring goals. Nonetheless, agencies have the option to acquire continuous monitoring tools that are not aligned with current or future CDM acquisition vehicles (CDM Dynamic and Evolving Federal Enterprise Network Defense [DEFEND], GSA IT Schedule 70 CDM Tools Special Item Number, etc.); however, agencies are required to provide sufficient justification prior to pursuing acquisition tools not aligned with the CDM program.[25] To do this, a justification memorandum must be sent from the agency CISO to the CDM PMO, the respective OMB Resource Management Officer (RMO), and OFCIO.

Agencies may continue to use their existing tools and capabilities (i.e., tools in place prior to the date of this memorandum) acquired outside of the CDM acquisition vehicles. Either way, agencies are still required to ensure their agency meets all of the Federal Dashboard reporting requirements. Agencies are encouraged to provide the CDM PMO feedback on existing tools and input on additional tools that may prove valuable for current or future CDM acquisition vehicles. When agencies exchange data with the Federal Dashboard they retain sole responsibility to respond to risks identified through the CDM program and/or its agency's dashboard.

Resource Allocations

When CDM PMO procures cybersecurity tools on behalf of an agency to fulfill specific CDM requirements, the CDM PMO will cover the license and maintenance costs of the base year and the maintenance for the first option year. Thereafter, CFO Act agencies are responsible for funding long-term operations and maintenance (e.g., licensing costs) of their CDM-related tools and capabilities. Agencies are required to submit separate, CDM-specific line items in their annual budget documents (see OMB Circular A-11), including the agency's congressional justification documents, as applicable. In addition, each agency should work with their OMB RMO to prepare a spend plan that details the resources (including estimated staff time) dedicated to CDM. Additionally, agencies shall, in coordination with their RMO, build CDM requirements into budget plans in future years. For non-CFO Act agencies, the CDM PMO will cover all costs when non-CFO Act agencies are unable to pay for CDM.[26]

Points of Contact

Agencies should direct questions about this memorandum and on information security program performance to OFCIO at ombcyber@omb.eop.gov.

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

Agencies should direct questions on CyberScope reporting to the CISA at FNR.FISMA@hq.dhs.gov.

---

[25] A justification should be provided for each contract period of performance to ensure existing tools keep pace with CDM contract vehicle tools.

[26] Non-CFO Act agencies must provide written justification to both OMB and CISA for approval.

Agencies should direct questions on FISMA metrics to OMB and CISA.

Agencies should direct questions on submission on potentially classified information to CISA at NCCIC@dhs.ic.gov with the subject line "FISMA 2021 Submission".

APPENDIX A: Additional CISA Responsibilities and Agency Implications

Scanning Internet Accessible Addresses and Systems

OMB directs CISA to take the following actions in the interest of improving Federal information security. These responsibilities are subject to OMB oversight and applicable FISMA requirements and limitations. In furtherance of those responsibilities and consistent with applicable law, regulation, policy, and existing Memoranda of Agreement with agencies, CISA 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.[27]

In order to ensure CISA can perform this function, each Federal civilian agency shall:

- Ensure that its standing Federal Network Authorization remains on file with CISA for incident response and hunt assistance;
- Ensure that an authorization remains on file with CISA for scanning of internet accessible addresses and systems, and that such authorization is reviewed semiannually; and,
- Provide, or continue providing, CISA 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.[28]
- Provide CISA with at least five business days advanced notice of changes to IP ranges by emailing vulnerability@cisa.dhs.gov.

Facilitating Information Sharing

To ensure that agencies can identify, detect, and respond to emerging malicious-actor tactics, techniques, and procedures (TTPs) all agencies must ensure that, at a minimum, the CIO and the CISO have Top Secret Sensitive Compartmented Information (TS-SCI) access. The TS-SCI clearance designation is necessary to view classified malicious-actor TTPs. Agencies experiencing challenges in attaining the required clearances for CIO and CISO officials should contact OMB for assistance in determining how best to ensure that these officials are cleared to perform required functions and duties, and fully participate in interagency information sharing.

---

[27] 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.

[28] 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).

APPENDIX B: FY 2020-2021 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 2020 FISMA CIO, Inspector General, and Senior Agency Official for Privacy metrics.	November 2, 2020	All agencies
#2	Provide agency annual report, including agency head letter, to Congress and the GAO.	No later than March 1, 2021	All agencies
#3	Update responses to FISMA CIO questions and metrics at least quarterly.	Quarter 1: no later than January 15, 2021	CFO Act agencies
		Quarter 2: no later than April 15, 2021	All agencies
		Quarter 3: no later than July 15, 2021	CFO Act agencies
		Quarter 4 / FY 2021 Annual: no later than October 29, 2021	All agencies
#4	Following the identification of an incident as "major," agencies shall: a. Notify affected individuals expeditiously as practicable, without unreasonable delay b. 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 agencies

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