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

October 25, 2018

THE DIRECTOR

M-19-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Mick Mulvaney
Director

SUBJECT: Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements

Purpose

This memorandum provides agencies with fiscal year (FY) 2019 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 into a single document 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-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*
- M-14-03, *Enhancing the Security of Federal Information and Information Systems*

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

Section I: Information Security 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) 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

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

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

CIO and IG Reporting: OMB and DHS will use both sets of metrics to compile the Annual FISMA Report to Congress and may use the CIO and IG reporting to compile agency-specific or 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, CIO Metrics are not limited to 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: 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]

[3] Chief Financial Officers Act of 1990, 31 U.S.C. § 901.

[4] 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 program structure, the dedicated resources, 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.

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

[6] 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.

- The Uniform Resource Locator (URL) for the agency's privacy program page,[7] as well as the URL for any other sub-agency-, component-, 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]

Table I provides the quarterly and annual reporting deadlines for remainder of FY 2018 and FY 2019.

Table I: Annual and Quarterly FISMA Reporting Deadlines

Reporting Period	Deadline	Responsible Parties
FY 2018 Annual CIO, IG, SAOP FISMA Reporting	October 31, 2018	All Agencies
FY 2019 Q1 CIO FISMA Reporting	January 15, 2019	CFO Act Agencies
FY 2019 Q2 CIO FISMA Reporting	April 16, 2019	All Agencies
FY 2019 Q3 CIO FISMA Reporting	July 17, 2019	CFO Act Agencies
FY 2019 Annual CIO, IG, and SAOP FISMA Reporting	October 31, 2019	All Agencies

II. Agency Head Letter for Annual Reporting Requirement to OMB

FISMA stipulates 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 shall 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 awareness and to validate the agency's FISMA report, OMB requires a signed letter from the agency head. In addition to the annual CIO, IG, and SAOP FISMA metrics, agencies must include 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:[9]

[7] 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 Personally Identifiable Information (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).

[8] Each agency is required to take steps to eliminate unnecessary collection, maintenance, and use of SSNs, and explore alternatives to the use of SSNs as personal identifiers. See OMB Circular A-130.

[9] 44 U.S.C. § 3554.

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 2018 government-wide targets in the CIO FISMA metrics;
B. Details on the total number of information security incidents reported to the National Cybersecurity and Communication Integration Center (NCCIC) through the DHS NCCIC Incident Reporting System,[10] and
C. 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 incident description to include attack vector, response, and remediation actions the agency has completed.

Reporting Method: Agencies must upload this letter to CyberScope as part of their annual reporting requirements. 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:[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, 2019**.[12]

[10] 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).
[11] 44 U.S.C. § 3554.
[12] OMB will not review, clear, or provide a template for the reports. Agencies should submit the reports directly to Congress and the GAO.

IV. High Value Assets List Updates

Identifying Federal High Value Assets (HVA's) has been a critical element of the Federal approach to managing cybersecurity risk since the establishment of the initiative in 2015. DHS and OMB continue to partner with agencies to refine the identification, categorization, and prioritization of HVAs across the Federal Government. As specified in Binding Operational Directive 18-02, in order to ensure effective identification and timely remediation of major (high) and critical weaknesses to HVA systems, all Federal agencies shall continue update their Points of Contact (POC's) Agency HVA submissions to DHS on a quarterly basis.

Agencies shall continue to abide by requirements established by BOD 18-02 and subsequent policy guidance provided by OMB.

As part of these requirements, each agency shall:

#	Action	Deadline
1	Review their Agency HVA list on a quarterly basis and provide updates and modifications via Homeland Security Information Network (HSIN).	FY 2018: October 31, 2018 Quarterly Reporting for FY 2019: Jan 15, April 16, July 17

Section II: Incident Reporting Requirements

Incident reporting is vital to understanding government-wide threats and aiding in incident response. Effective incident reporting provides government-wide insight on attack vectors, time to detect, and time to restore operations. Agencies must report incidents to DHS NCCIC according to the current and updated requirements in the NCCIC Federal Incident Notification Requirements[13]

OMB is providing the following guidance to assist agencies in submitting incident response data and to promote coordination 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. 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.

[13] Required by 44 U.S.C. § 3554(b)(7)(C)(ii)

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.[14] 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*.

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.[15]

A major incident determination is required for any unauthorized modification of any unauthorized modification of, [16] unauthorized deletion of,[17] unauthorized exfiltration of,[18] or unauthorized access to[19] the PII of 100,000 or more people. Agencies should assess each breach on a case-by-case basis to determine whether the breach meets the definition of a major incident. 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 DHS and OMB to make a major incident determination.

[14] Using the NCCIC's 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 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."

[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*, which describes breach reporting requirements.

[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.

Reporting Major Incidents

I. Reporting to DHS and OMB.

- Agencies must report to DHS NCCIC and the OMB Office of the Federal Chief Information Officer (OFCIO) within one hour of determining an incident or breach to be a major incident, and should update NCCIC and OMB OFCIO within one hour of determining that an already-reported incident or breach has been determined to be a major incident.[20]
- 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 has a reasonable basis to conclude that a major incident, or that a breach constituting 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.

[20] This reporting is limited to the time after major incident determination 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”.

[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).

- 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 a breach constituting a major incident.[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.

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 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.[23]

Each Federal civilian agency shall:

- 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,
- Provide, or continue providing, DHS a complete list of all internet-accessible Federal information systems and related addressing information semiannually, including static

[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] 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.

internet protocol (IP) addresses for external websites, servers, and other access points and domain name service names for dynamically provisioned systems.[24]
- Provide DHS with at least five business days advanced notice of changes to IP ranges by emailing NCATS@hq.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.

Reporting a Breach to US-CERT

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.

Section III: Strengthening Continuous Diagnostics and Mitigation Capabilities

This section supersedes the program and reporting requirements in OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*, and rescinds that memorandum.

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 allows agencies to effectively monitor, defend, and rapidly respond to cyber incidents.

The DHS 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.

[24] 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).

While the DHS 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 DHS in order to accomplish CDM program goals at the agency level.

CDM Implementation & Agency Responsibilities and Expectations

Federal Dashboard Deployment and Operations

DHS will maintain a fully operational Federal Dashboard to provide situational awareness of the Federal Government's overall cybersecurity posture. A fully-operational Federal Dashboard means any federal agency ready to exchange data with the Federal Dashboard will be able to do so and technical capabilities for operating and maintaining the Federal Dashboard are in-place. Both CFO and non-CFO Act agencies shall establish the information exchange between their respective agency dashboards and the Federal Dashboard according to the timeline set forth by the CDM PMO.

DHS, in consultation with OMB, will specify the data attributes agencies are required to supply to the Federal Dashboard in the CDM Technical Requirements Document, and will circulate updates to the document by Q3 of each Fiscal Year. DHS, in consultation with OMB, will review technical and data attributes as necessary and DHS will update the Technical Requirements Document accordingly.

Acquiring Capabilities

CDM currently provides agencies with a cost-effective and efficient strategy for achieving government-wide information security continuous monitoring goals. Nonetheless, agencies may acquire continuous monitoring tools outside of this program; however, they are required to provide sufficient justification should they pursue acquisition of tools with continuous monitoring capabilities that are not aligned with current or future CDM acquisition vehicles (includes CDM Dynamic and Evolving Federal Enterprise Network Defense [DEFEND], GSA IT Schedule 70 CDM Tools Special Item Number, etc.). Prior to purchasing these tools, a justification memorandum must be sent from the agency CISO to the CDM PMO, the respective OMB Resource Management Office (RMO), and the Office of the Federal Chief Information Officer (OFCIO) Cybersecurity Team.

Agencies may continue using existing tools and capabilities (i.e., tools in-place prior to publication of this memorandum) acquired outside of the CDM acquisition vehicles, and will need to ensure the agency meets all CDM reporting requirements to the Federal Dashboard. 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, agencies retain sole responsibility to respond to risks identified through the CDM program and/or its agency's dashboard.

Resource Allocations

For cybersecurity tools the CDM PMO procures on behalf of an agency to fulfill specific CDM requirements, the CDM PMO will cover the license and maintenance cost of the base year and the maintenance for the first option year. Agencies are then 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 FY 2021 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 from FY 2018 through FY 2021. Additionally, agencies shall, in coordination with their RMO, build CDM requirements into budget plans beyond FY 2021.

Section IV: Implementing the Federal Cybersecurity Risk Determination Report and Action Plan

In May 2018, OMB released the Federal Cybersecurity Risk Determination Report and Action Plan in accordance with Executive Order 13800, which provides a comprehensive assessment of government cybersecurity risk management challenges, and identifies actions to improve Federal cybersecurity. This memorandum addresses two of the actions from the Report:

a. Consolidate agency Security Operations Centers (SOCs)[25] to improve incident detection and response capabilities; and
b. Increase cybersecurity threat awareness among Federal agencies by implementing the Director of National Intelligence's (ODNI) Cyber Threat Framework to prioritize efforts and manage cybersecurity risks.

Security Operations Center Consolidation

A major finding of the Risk Determination Report and Action Plan was that a majority of agencies lack sufficient visibility into what is occurring on their network. To improve, and centralize visibility, OMB and DHS will work with agencies to assess and enhance the maturity of their SOCs and streamline security operations across their enterprise. To this end, each agency shall:

[25] Pursuant to the Federal Security Operations Center Best Practices, a SOC defends an organization against unauthorized activity within computer networks, including, at a minimum, detecting, monitoring, and analyzing suspicious activity as well as leading the response to malicious activity, contributing to restoration activities, and providing a structure for users to report suspected cybersecurity events. A SOC would generally be composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

#	Action	Deadline
1	Develop and submit one enterprise-level Cybersecurity Operations Maturation Plan to OMB and DHS, including a justification for the approach detailed by the plan. The plan is should be based on data submitted through the agency's FY2020 Budget Data Request on Government-wide Tracking of Resources for Cyber Activities (Cyber BDR).[26] Required content for the plan can be found in Appendix B.	April 16, 2019
2	Complete SOC Maturation, Consolidation or Migration to SOC as a Service	September 30, 2020

This plan should be developed and formally submitted by the agency's CISO and, prior to submitting the plan, the CISO must consult with the agency's Chief Information Officer (CIO), Chief Financial Officer (CFO), Chief Human Capital Officer (CHCO), and Chief Procurement Officer (CPO) or their respective equivalents.

The plan must:

- provide a description and diagram of the current-state operating model of enterprise-wide cybersecurity operations;
- detail the agency's approach to enhancing the maturity of enterprise-wide cybersecurity operations, whether through SOC consolidation and process improvement, migration to a service provider, or a combination of the two;
- list the affected policies, processes, facilities, teams, contracts, budget accounts, or any other matters deemed pertinent to this initiative;
- include a description and diagram of the end-state operating model of enterprise-wide cybersecurity operations;
- articulate a timeline of immediately executable actions, such as defining and coordinating a governance structure, identifying resource requirements, or conducting any relevant planning activities;
- outline actions that are dependent on current and future funding and cannot be taken immediately, including a proposed timeline for their implementation;
- summarize activities and milestones related to sustaining and continuously improving the agency's enterprise-wide cybersecurity operating model moving forward.

Cyber Threat Framework Implementation

The Risk Determination Report and Action Plan found that Agencies do not understand how threat actors seek to gain access to their networks, systems, and data, leading to ineffective allocations of agencies' limited cyber resources. The Report promotes the use of the ODNI

[26] Please refer to p. 59-61 of *FY2020 IT Budget – Capital Planning Guidance*, available at: https://www.whitehouse.gov/wp-content/uploads/2018/06/fy-2020-it-budget-guidance.pdf

Cyber Threat Framework, which provides a common language for describing and communicating information about cyber threat activity. To foster the adoption of the Cyber Threat Framework across the government, DHS in coordination with OMB and DoD, shall:

#	**Action**	**Deadline**
1	Develop and implement a solution that leverages threat intelligence to identify deficiencies in agency security capability coverage against adversarial activity (e.g. heat mapping).	April 30, 2019
2	Support agencies in identifying and assessing their security capability coverage on High Value Assets	October 31, 2019
3	Enable agencies to use the solution to prioritize cybersecurity investments based on threat-informed risk management, with specific focus on HVAs	December 31, 2019

Points of Contact

Agencies should direct questions about this memorandum and 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) Privacy Branch 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: Agencies Required to Participate in the HVA Program

This Appendix documents the civilian agencies within the Federal Executive branch that are required to participate in the HVA Program outlined in OMB Memoranda and DHS BODs. This includes the bureaus / components / organizations that are subsidiaries of the Federal Civilian agencies mentioned. Though an agency's Office of the Inspector General (OIG) operates an independent network and often participates in DHS activities independently of the parent agency, this list incorporates OIG systems into the parent agency for purposes of required reporting and program agreements.

#	Federal Agency Name	Acronym
1	Administrative Conference of the United States	ACUS
2	Advisory Council on Historic Preservation	ACHP
3	African Development Foundation	ADF
4	American Battle Monuments Commission	ABMC
5	Barry M Goldwater Scholarship Foundation	BGSF
6	Broadcasting Board of Governors	BBG
7	Chemical Safety Board	CSB
8	Christopher Columbus Fellowship Foundation	CCFF
9	Commission of Fine Arts	CFA
10	Commodity Futures Trading Commission	CFTC
11	Consumer Financial Protection Bureau	CFPB
12	Consumer Product Safety Commission	CPSC
13	Corporation for National and Community Service	CNCS
14	Council of the Inspectors General on Integrity and Efficiency	CIGIE
15	Court Services and Offender Supervision Agency for the District of Columbia	CSOSA
16	Defense Nuclear Facilities Safety Board	DNFSB
17	Denali Commission	DENALI
18	Department of Commerce	DOC
19	Department of Education	ED
20	Department of Energy	DOE
21	Department of Health and Human Services	HHS
22	Department of Homeland Security	DHS
23	Department of Housing and Urban Development	HUD
24	Department of the Interior	DOI
25	Department of Justice	DOJ
26	Department of Labor	DOL
27	Department of State	DOS
28	Department of Transportation	DOT
29	Department of the Treasury	TREAS
30	Department of Veterans Affairs	VA
31	Election Assistance Commission	EAC

#	Federal Agency Name	Acronym
32	Environmental Protection Agency	EPA
33	Equal Employment Opportunity Commission	EEOC
34	Export-Import Bank of the United States	EXIM
35	Farm Credit Administration	FCA
36	Farm Credit System Insurance Corporation	FCSIC
37	Federal Communications Commission	FCC
38	Federal Deposit Insurance Corporation	FDIC
39	Federal Energy Regulatory Commission	FERC
40	Federal Financial Institutions Examination Council (including FFIEC Appraisal Subcommittee)	FFIEC and ASC
41	Federal Housing Finance Agency	FHFA
42	Federal Labor Relations Authority	FLRA
43	Federal Maritime Commission	FMC
44	Federal Mediation and Conciliation Service	FMCS
45	Federal Mine Safety and Health Review Commission	FMSHRC
46	Federal Reserve Board of Governors	FRB
47	Federal Retirement Thrift Investment Board	FRTIB
48	Federal Trade Commission	FTC
49	General Services Administration	GSA
50	Gulf Coast Ecosystem Restoration Council	GCERC
51	Harry S. Truman Scholarship Foundation	HTSF
52	Institute of Museum and Library Services	IMLS
53	Inter-American Foundation	IAF
54	U.S. Section of International Boundary and Water Commission	IBWC
55	James Madison Memorial Fellowship Foundation	JMMFF
56	Marine Mammal Commission	MMC
57	Merit Systems Protection Board	MSPB
58	Millennium Challenge Corporation	MCC
59	Morris K. Udall and Stewart L. Udall Foundation	UDALL
60	National Aeronautics and Space Administration	NASA
61	National Archives and Records Administration	NARA
62	National Capital Planning Commission	NCPC
63	National Council on Disability	NCD
64	National Credit Union Administration	NCUA
65	National Endowment for the Arts	NEA
66	National Endowment for the Humanities	NEH
67	National Labor Relations Board	NLRB
68	National Mediation Board	NMB
69	National Science Foundation	NSF
70	National Transportation Safety Board	NTSB

#	Federal Agency Name	Acronym
71	Nuclear Regulatory Commission	NRC
72	Nuclear Waste Technical Review Board	NWTRB
73	Occupational Safety and Health Review Commission	OSHRC
74	Office of Government Ethics	OGE
75	Office of Navajo and Hopi Indian Relocation	ONHIR
76	Office of Personnel Management	OPM
77	Office of Special Counsel	OSC
78	Overseas Private Investment Corporation	OPIC
79	Peace Corps	PC
80	Pension Benefit Guaranty Corporation	PBGC
81	Postal Regulatory Commission	PRC
82	Presidio Trust	PT
83	Privacy and Civil Liberties Oversight Board	PCLOB
84	Railroad Retirement Board	RRB
85	Securities and Exchange Commission	SEC
86	Selective Service System	SSS
87	Small Business Administration	SBA
88	Social Security Administration	SSA
89	Social Security Advisory Board	SSAB
90	Surface Transportation Board	STB
91	Tennessee Valley Authority	TVA
92	United States AbilityOne Commission	USAC
93	United States Access Board	USAB
94	United States Agency for International Development	USAID
95	United States Commission on Civil Rights	USCCR
96	United States Department of Agriculture	USDA
97	United States Interagency Council on Homelessness	USICH
98	United States International Trade Commission	USITC
99	United States Trade and Development Agency	USTDA
100	Vietnam Education Foundation	VEF

APPENDIX C: FY 2018-2019 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 2018 FISMA CIO, Inspector General, and Senior Agency Official for privacy metrics.	October 31, 2018	All agencies
#2	Provide agency annual report, including agency head letter, to Congress and the GAO.	No later than March 1, 2019	All agencies
#3	Update responses to FISMA questions and metrics at least quarterly.	Quarter 1: no later than January 15, 2019	CFO Act agencies
		Quarter 2: no later than April 16, 2019	All agencies
		Quarter 3: no later than July 17, 2019	CFO Act agencies
		Quarter 4 / FY 2019 Annual: no later than October 31, 2019	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	Ongoing	All agencies

	designated as sensitive positions and the incumbents have Top Secret Sensitive Compartmented Information access.		
#6	Submit separate, CDM-specific line items in all future budget documents, including the agency's congressional justification documents and spend plan, as applicable.	Beginning in FY 2020	All agencies
#7	Develop and submit one enterprise-level Cybersecurity Operations Maturation Plan to OMB and DHS, including a justification for the approach detailed by the plan. This plan should include, but is not limited to, a timeline of actions and milestones required for the agency to consolidate its Security Operations Centers by September 30, 2020.	April 16, 2019	All agencies
#8	Complete SOC Consolidation or Migration to SOC as a Service	September 30, 2020	All agencies
#9	Review the Agency HVA list on a quarterly basis and provide updates and modifications via HSIN.	Next date: October 31, 2018	All agencies
#10	Develop and implement a solution that leverages threat intelligence to identify gaps in agency security capability coverage (i.e. heat mapping).	April 30, 2019	CFO Act Agencies
#11	Support agencies in identifying and assessing their security capability coverage on High Value Assets	October 31, 2019	CFO Act Agencies
#12	Enable agencies to use the solution to prioritize cybersecurity investments based on threat-informed risk management, with specific focus on HVAs	December 31, 2019	CFO Act Agencies