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

THE DIRECTOR

January 15, 2025

M-25-04

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young Shalanda D. Young
Director

SUBJECT: Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements

Purpose

This memorandum provides agencies with Fiscal Year (FY) 2025 reporting guidance and deadlines in accordance with the Federal Information Security Modernization Act (FISMA) of 2014 (FISMA).[1] It rescinds the following memoranda:

- M-24-04, *Fiscal Year 2024 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 this guidance to inform agency national security system management processes.

Introduction

In FY 2024, agencies continued to make progress implementing the bold changes and significant investments the President outlined in Executive Order 14028, *Improving the Nation's Cybersecurity* (EO 14028) and its implementation memos, particularly the Federal Zero Trust Strategy (OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*), by increasing deployment of critical security tools throughout the Federal enterprise and rethinking fundamental approaches to cybersecurity.

Additionally, the release of the National Cybersecurity Strategy (NCS) in March 2023 has been a catalyst for continued agency improvement. The Office of the National Cyber Director (ONCD) updated the NCS Implementation Plan (NCSIP) in May 2024 to improve the resilience of critical

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

infrastructure, apply the National Cyber Workforce and Education Strategy, and expand agency initiatives to disrupt threat actors.

To ensure agencies prioritize cybersecurity efforts aligned with E.O. 14028, the NCS, and the Office of Management and Budget (OMB) cyber policy guidance, OMB and ONCD jointly released OMB Memorandum M-24-14, *Administration Cybersecurity Priorities for the FY 2026 Budget* in July 2024. Because Federal agencies have finite resources to dedicate to cybersecurity, they must focus those resources on activities such as continuing to mature zero trust architectures that are critical to mitigating cybersecurity risks. Agencies are expected to incorporate performance measurement strategies into resource requests in order to build visibility in requested activities and allow effective measurement of investments. OMB will continue to leverage the budget process to assess agency alignment to the Administration's cyber priorities.

The guidance within this memorandum continues this Administration's effort to leverage data collected from agency FISMA submissions to improve the security outcomes of federal IT systems, as articulated in the National Cyber Strategy's call to modernize systems and continue to build our collective defense:

Improving agency's secure cloud adoption: As described in OMB Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*, the purpose of FedRAMP is to increase Federal agencies' adoption and secure use of the commercial cloud, by providing a standardized reusable approach to security assessments and authorizations for cloud computing products and services. Modernizing FedRAMP to meet the needs of agencies and assist them in selecting and adopting cloud solutions with appropriate safeguards for the security of the information they process will enable the Federal Government to safely use the best of the commercial cloud marketplace for years to come. To assist in evaluating that adequate security is in place, the FedRAMP Marketplace data has been automated into FISMA reporting in order to compile a comprehensive baseline inventory of the cloud services being utilized by Federal agencies.

Measuring zero trust implementation: Agencies are required to sustain efforts in support of continued implementation of E.O. 14028, including continuously increasing the maturity of their Zero Trust posture. OMB has worked with agency chief information officers (CIOs) and chief information security officers (CISOs), as well as the Cybersecurity and Infrastructure Security Agency (CISA), to ensure that metrics used in FISMA data collection align with these priorities. OMB will continue to align performance management under FISMA with benchmarks for the implementation of National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the agency's zero trust implementation strategy. This effort is critical for future metric development.

Enhancing the Security of the Software Supply Chain: Following E.O. 14028, OMB issued guidance through OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* and OMB Memorandum M-23-16, *Update to M-22-18* which required agencies to collect attestations from software producers that affirm compliance with minimum secure software development practices. M-22-18 and M-23-16 seek to enhance the fidelity of software used by agencies to achieve their mission goals, ultimately enabling the secure delivery of government services to the public. The quantification of this effort is reflected in new FISMA metrics that aim to track agency implementation maturity.

Clear, actionable, and outcome-focused data: To ensure agencies can continue to focus on outcomes over manual reporting, the FY 2025 CIO metrics will continue to expand on the work over the past several fiscal years to improve the automated reporting of agency information security metrics. Even where full automation is not yet achievable, this memorandum requires agencies and CISA to provide performance and incident data to OMB in a machine-readable format. OMB intends for agencies to focus and prioritize their limited resources on collection efforts for data elements that provide critical insight into their security risk posture.

Ensuring input from across the Federal enterprise: Building on the progress made over the past two fiscal years, OMB and CISA will continue to support the efforts of the Federal Chief Information Security Officer Council's FISMA Metrics Subcommittee. The purpose of the FISMA Metrics Subcommittee is to analyze FISMA guidance and metrics and provide OMB with recommendations regarding refinements and improvements to the guidance and metrics for the following fiscal year. OMB and the subcommittee reviewed the following in FY 2024 and will continue to support implementation of these areas in FY 2025:

- Prioritizing automation of specific metrics for FY 2025 and beyond, including supporting agencies to prepare for the necessary processes to ensure accurate data;
- Incorporating Continuous Diagnostic and Mitigation (CDM) data into FISMA reporting;
- Improving the evaluation criteria and subsequent determination of effectiveness by agency IGs;
- Recommending additional methodologies to capture information regarding agency risk-based decisions and mitigations, as well as agencies' reliance upon authorized exceptions to or waivers from the requirements of OMB policies and CISA Emergency Directives and Binding Operational Directives (BODs);
- Improving how the effectiveness of Federal agency information security programs are measured;
- Ensuring reporting of accurate and valid data, in part through the use of standard nomenclature;
- Working with the National Institute of Standards and Technology (NIST) and CISA to align the Zero Trust Maturity Model v2.0 (ZTMM), and any subsequent updated model, with the Cyber Security Framework v2.0 (CSF) by the end of FY 2025; and
- Maturing the current and future metrics used to measure implementation of Zero Trust principles.

Supporting security-privacy coordination: While security and privacy are independent and separate disciplines, they also have a close relationship.[3] Security and privacy planning, monitoring, and reporting are increasingly integrated, and agencies continue to benefit from increased collaboration and coordination across these disciplines. This coordination is essential to managing security and privacy risks and to complying with applicable requirements,[4] including those outlined in this memorandum. For example, when a breach[5] occurs, such coordination is critical, and this memorandum underscores the guidance provided on roles regarding tracking and documenting the breach in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

Improving incident response: This memorandum builds on Administration efforts to ensure CISA works closely with Federal agencies in building a cohesive, coordinated incident response infrastructure. E.O. 14028 laid out a series of actions to modernize the Federal Government's investigative and remediation capabilities. If incidents are not properly reported – or subsequent updates regarding the incident are improperly documented – the detection, investigation, and remediation of sophisticated cyber threats may suffer. Therefore, agencies should take steps to reduce their mean times to detect, analyze, respond, and recover. Improving agency performance for incident response requires a multi-faceted and sustained approach that agencies should tailor to the specific challenges that have historically prevented improvement in these areas. This includes process improvements, enhanced tooling, automation, proactive alerting, and systematically capitalizing on lessons learned. Agencies can work with CISA and other third parties to evaluate their tactical and strategic approaches to incident response management.

Section I: Responsibilities of the Cybersecurity and Infrastructure Security Agency

CISA's Continuous Diagnostics and Mitigation (CDM) Program

The CDM program allows Federal agencies to monitor vulnerabilities and threats to their systems in near real-time. This increased situational awareness helps agencies prioritize actions to mitigate or accept cybersecurity risks. The CDM program works with agencies to deploy commercial off-the-shelf tools that provide enterprise-wide visibility of assets, users, and activities. This enables agencies to more effectively monitor, defend, and 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[6] 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 responsible for the state of their

[3] OMB Circular A-130, Managing Information as a Strategic Resource, § 4(h) (July 28, 2016).

[4] *Id.*

[5] The term "breach" is defined in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, § III(C) (Jan. 3, 2017). This definition applies to the term "breach" throughout this memorandum.

[6] The CFO Act agencies are defined in 31 U.S.C. § 901(b).

cybersecurity posture and must work closely with CISA to accomplish CDM program goals within their own enterprises. CISA will continue to provide OMB with monthly data on implementation progress by all Federal agencies.

CDM Implementation and Agency Responsibilities and Expectations

Automated Reporting: Agencies are required to report at least 90 percent of Government-furnished equipment (GFE) through the CDM program inclusive of their Endpoint Detection and Response (EDR) tool deployment, as articulated in previous FISMA guidance and aligning with requirements of BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks.* CISA will continue to provide OMB with performance data, including information on scanning cadence, rigor, and completeness of vulnerability enumeration as part of the FY 2024 metrics collection process. Beginning in FY 2025, CISA will begin examining the capabilities called for in M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, to automatically capture the number of endpoints running EDR tools, and compare this to data manually reported in CyberScope. This comparison will be used to improve the accuracy of automated data capture with the intent of alleviating the manual reporting burden in future reporting years. Agencies must continue to provide data on assets in an automated manner to the maximum extent feasible. This is supported by the adoption throughout each agency of CDM and other technical solutions that provide visibility and automated reporting directly to CISA. The CISO Council FISMA Metrics Subcommittee should continue to identify future metrics for automation in FY 2025. As fully automated identification of certain non-conforming assets through CDM may not be feasible, agencies must continue to report their own asset counts through CyberScope. It is imperative that Federal agencies regularly evaluate their CDM datasets and ensure unmanaged devices detected by tools and sensors are appropriately managed, categorized, and assignments made to systems, as appropriate.

Acquiring Capabilities: Although agencies may acquire continuous monitoring tools through means other than 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.), agencies must provide sufficient justification before pursuing acquisition tools not aligned with the CDM program.[7] A justification memorandum must be sent from the agency CISO to the CDM PMO, the relevant OMB Resource Management Office (RMO), and the OMB Office of the Federal Chief Information Officer (OFCIO) for concurrence. OMB may reevaluate agency justification memoranda.

Agencies must meet all of the CDM Federal Dashboard reporting requirements. Further, when agencies exchange data with the Federal Dashboard, they are responsible for responding to risks

[7] A justification should be provided from the agency CISO to the CDM PMO, the relevant OMB Resource Management Officer, and the OMB Office of the Federal Chief Information Officer for each contract period of performance to ensure existing tools keep pace with CDM contract vehicle tools.

identified through the CDM program and the agency dashboard. Agencies are encouraged to provide the CDM PMO with feedback on existing tools and input on additional tools that may prove valuable for current or future CDM acquisition vehicles.

Resource Allocations: When the CDM PMO procures cybersecurity tools on behalf of an agency to fulfill specific CDM requirements, the PMO will cover the license and maintenance costs of the base year and the maintenance cost for the first option year. Otherwise, CFO Act agencies are responsible for the operations and maintenance costs (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 their congressional justification documents, as applicable. In addition, each agency should work with its OMB RMO to prepare a spending plan that details the resources (including estimated staff time) dedicated to CDM. Each agency shall, in coordination with its RMO, build CDM requirements into budget plans in future years. For non-CFO Act agencies that are unable to pay for CDM, the CDM PMO will cover all costs.[8]

Section II: Internet of Things and Operational Technology

Agencies must have a clear understanding of the devices connected within their FISMA systems to have a clear understanding of their cybersecurity risk. This includes the networked internet of things (IoT) and operational technology (OT) devices that interact with the physical world—from building maintenance systems, to environmental sensors, to specialized equipment in hospitals and laboratories.

Maturing the cybersecurity posture of IoT and OT devices within the federal enterprise requires that we ensure foundational cyber protection measures are in place for all such devices connected to federal systems. The prevalence and wide range of IoT and OT devices used by Federal agencies provides new and more complex vectors for cyber incidents. By prioritizing a well-planned and iterative maturation process, we can move toward ensuring the resilience and trustworthiness of these technologies.

The Internet of Things Cybersecurity Improvement Act of 2020[9] (IoT Act) required the National Institute of Standards and Technology (NIST) to publish guidelines and standards[10] for: (1) the appropriate use by Federal agencies of Internet of Things (IoT) devices; and (2) addressing and sharing information about the security vulnerabilities of those devices.[11]

Following significant engagement with stakeholders and recognizing the vulnerabilities to federal systems complex IoT devices may create, this memorandum is providing additional guidance on identifying and securing such devices.

Scoping and Definitions of Operational Technology and Internet of Things Devices

[8] Non-CFO Act agencies must provide written justification to both OMB and CISA for approval.
[9] Pub. L. No. 116-207 (2020), *codified at* 15 U.S.C. §§ 278g-3a to -3d.
[10] SP 800-213 and SP 800-213A.
[11] 15 U.S.C. §§ 278g-3b(a)(1), 278g-3c(a).

NIST defines IoT devices as those that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world.[12]

OMB has engaged with agencies about the diversity of "smart" devices prevalent throughout the federal government. Due to the wide range of devices this definition encompasses and the complexity, for the purposes of this guidance, IoT devices refers to embedded programmable controllers, integrated circuits, sensors, and other technologies for the purpose of collecting and exchanging data with other devices or systems over a network in order to facilitate enhanced connectivity, automation, and data-driven insights across devices and systems. This guidance is relevant to any and all such devices within FISMA system boundaries.

When referring to Operational Technology, this guidance refers to the following NIST definition: **"**Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms."[13]

IoT and OT Inventory

Inventorying of agency IoT and OT technology assets is critical for ensuring the cybersecurity posture of an enterprise, as these assets are increasingly interconnected with IT hardware and software. An inventory is necessary for agency CIOs and CISOs to gain visibility over their connected devices and systems, apply appropriate controls (such as those set out in NIST SP 800-213 and NIST SP 800-82 and for IOT and OT, respectively), and make risk-based decisions about mitigating against cybersecurity incidents. Additionally, an inventory enables more efficient identification and patching of vulnerabilities to ensure a more secure and resilient infrastructure. Inventorying is also a necessary prerequisite to establishing a baseline to enable monitoring and detecting unauthorized, abnormal, or potentially malicious activities.

To enhance the U.S. Government's overall cybersecurity posture and to help ensure integrity of systems, agency CIOs shall work with asset owners and operators to maintain an updated, enterprise-wide inventory inclusive of their agency's IoT and OT assets. Inventories must include the following information:

1) Asset Identification: All devices and systems that meet the provided definition of IoT or OT.
2) Asset Description: Including make, model and any relevant specifications or configurations. Each asset should have a unique identifier, such as a serial or asset tag, to distinguish it from other assets.

[12] NISTIR 8425
[13] NIST SP 800-37, Rev. 2

3) Asset Categorization: Factor in the device’s function, location, and criticality. Include the following information:
    a. Identification and/or description of specific agency FISMA and HVA systems associated with the asset; and
    b. The physical location of the asset, (e.g., facility ID) if practicable via the hardware asset management tool.
4) Information System Owner/ISSO: The individual or office responsible for the asset’s management, administration, maintenance, and security.
5) Vendor/Manufacturer Information: Include details about the vendor or manufacturer (e.g., contact information and support channels.)
6) Software and Firmware Versions: Record the installed software and firmware versions, including relevant patches or updates applied to the asset.
7) Network Connectivity, Integrations and API Information: Specify network connection details, such as ports used by the asset (e.g., software-based integrations and application programming interfaces.)
8) Security Controls: Describe physical and technological security controls (e.g., user accounts and permissions, encryption of data at rest and in transit, physical controls, and authentication methods.)

Agency inventories meeting other widely-accepted security guidelines, standards, or regulatory frameworks are acceptable in lieu of the above requirement so long as they include the above data points.

IoT and OT devices have varying risk profiles and levels of criticality to agency missions. Agencies shall prioritize the inventorying of assets that:

1) Are in the critical path for mission-enabling functions,
2) Are located in networked environments where they may act as an initial access vector, or
3) Communicate or collect sensitive data.

CIOs must work with agency IoT and OT system owners and operators to document critical paths for mission-enabling functions, as well as the related systems, processes, and assets upon which those functions depend. As part of this process, teams should also evaluate critical attack or disruption pathways adversaries could leverage to compromise critical devices and connected IT systems. This data should be used for prioritizing risk mitigation.

IoT Procurement Waiver Process

The Internet of Things Cybersecurity Improvement Act of 2020[14] (IoT Act) required the National Institute of Standards and Technology (NIST) to publish guidelines and standards[15] for: (1) the appropriate use by Federal agencies of Internet of Things (IoT) devices; and (2) addressing and

[14] Pub. L. No. 116-207 (2020), *codified at* 15 U.S.C. §§ 278g-3a to -3d.
[15] SP 800-213 and SP 800-213A.

sharing information about the security vulnerabilities of those devices.[16] Those standards and guidelines apply to any Federal entity that qualifies as an “agency” within the meaning given in 44 U.S.C. § 3502(1).

The IoT Act also specifies particular implementation measures for CFO Act agencies, other than the Department of Defense. Before any CFO Act agencies may enter into a contract for IT or IT services, the agency CIO must review and approve the contract, as required by 40 U.S.C. § 11319(C)(i)(I). Under the IoT Act, if the CIO conducts such a review of a contract for an IoT device, and determines during that review that using the device would prevent the agency from complying with NIST’s IoT standards and guidelines, then the agency is prohibited from using the device, procuring, or obtaining the device, or renewing a contract to procure or obtain the device.[17]

That prohibition may be waived, but only if the agency CIO first determines that at least one of the following conditions is met:

1) The waiver is necessary in the interest of national security;
2) Procuring, obtaining, or using the IoT device is necessary for research purposes; or
3) The device is secured using alternative and effective methods appropriate to its function.[18]

The CIO shall memorialize and justify any such determination in a signed memorandum for the agency head. Upon receiving that memorandum, the agency head may issue an *IoT Procurement Waiver* of the prohibition on use or acquisition of the device in question. The waiver must include the following, at a minimum:

1) Date of issuance;
2) The device(s) and any associated solutions or platforms covered;
3) A description of the purposes for which or the circumstances in which the device may be acquired or used.
4) The effective period of the waiver, which may not exceed 2 years;
5) A copy of the memorandum setting out the CIO’s determination; and
6) The signature of the agency head or their designee.

A copy of any *IoT Procurement Waiver* signed by the agency head must be provided to the agency CIO. CIOs must make these waivers available to OMB upon request, and ensure that such waivers are documented in relevant system security plans. Agencies should regularly review, at least annually, to ensure such waivers are still necessary and reasonable and shared with acquisition officials for documentation in relevant contract files. OMB has determined no additional policies or clarifications are required at this time for agencies to implement this waiver process.

[16] 15 U.S.C. §§ 278g-3b(a)(1), 278g-3c(a).
[17] 15 U.S.C. § 278g-3e(a).
[18] *Id.* § 278g-3e(b)(1).

IoT and OT Security Risk Management

When system owners determine a Federal information system containing IoT or OT devices cannot support specific mandated IT controls, they should implement appropriate compensating controls to mitigate the same risk as the mandated IT control. For example, if systems with IoT or OT devices cannot reasonably accommodate multi-factor authentication, systems owners should implement compensating controls to minimize the risk of authentication vulnerabilities such as weak or stolen credentials.

Systems containing IoT devices should be secured to the maximum extent feasible outlined by NIST IR 8228 and the NIST SP 800-213 series. Similarly, systems containing OT devices should be secured to the maximum extent feasible as outlined by NIST SP 800-82 rev. 3, or any successor publication.

Authorizing officials must document the risk-based decision to secure systems with IoT or OT devices to the maximum extent feasible using compensating controls instead of the mandated IT controls. The documentation shall include the following information:

1) Justification for not implementing the mandated IT control (e.g., technology does not exist or is too expensive.)
2) Risk determination (e.g., results of a risk assessment)
3) Risk response (e.g., avoidance, mitigation, transference, decision, or implementation)
4) Risk monitoring (e.g., verifying compliance, determine ongoing effectiveness of risk response, and identify risk-impacting changes to the organization or environment)

All systems which include an IoT device with an approved *IoT Procurement Waiver* must also complete aforementioned risk-based decision documentation. All risk-based decision documentation shall be made available to OMB upon request.

Section III: Cybersecurity Logging

Following E.O. 14028, OMB issued guidance through OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, which established agency requirements for logging and log retention and management, with a focus on ensuring centralized access and visibility for the highest level security operations center (SOC) of each agency. M-21-31 underscores the importance of data from network and system logs in helping agencies detect cyber threats and investigate cyber incidents. Effective cybersecurity risk management requires continuous evolution and dynamic strategies to address the fast-paced growth of new technologies and threats. Requirements such as cybersecurity event logging can aid agencies in continuously measuring and effectively mitigating cybersecurity risk in a manner that is scalable, risk-centric, and maximizes utilization of existing resources and environments.

To further improve vulnerability and incident detection, CISA, in coordination with OMB, will provide a reference architecture on the use of logging capabilities for proactive continuous event monitoring. The document will prioritize the following two critical security objectives to ensure investigative readiness:

- **Logging for Continuous Event Monitoring (CEM):** Logs, log management, and logging infrastructure enabling the proactive and near real-time continuous monitoring of security events for the purpose of detecting cybersecurity events with live analysis, typically carried out through the monitoring functions of a SOC.

- **Logging for Response, Investigation, and Forensics (RIF):** Logs, log management, and logging infrastructure enabling reactive response (to include containment and remediation), investigation, and/or forensics for the purpose of recovery, mitigation, inspection, investigation, and remediation of the impact of an incident as well as retention requirements by statute or regulation. This includes but is not limited to investigation of a root cause of incident/failure and/or forensic analysis.

The reference architecture shall also include a model for agencies to conduct self-assessments on their logging capabilities. Agencies should use this reference architecture as a central, dynamic source for logging related security objective achievement and implementation details. CISA will update this reference architecture regularly to account for new or evolved cybersecurity event logging and log management best practices.

Where agency data is otherwise subject to statutory, regulatory, or judicial access restrictions, CISA will comply with agency processes and procedures required to access such data or work with the agency to develop an appropriate administrative accommodation consistent with any such restriction to ensure that the data is not subject to unauthorized access or use.

CISA Responsibilities:

- In coordination with OMB, provide a reference architecture on logging best practices, including CEM and RIF, by April 30, 2025.
- Coordinate with the interagency enterprise logging working group to evaluate and, if necessary, update the reference architecture at a minimum of annually.
- Provide logging implementation technical support and advisement to agencies via frequently asked questions, interagency engagements (e.g., workshops, focus groups, communities of practice), training, and direct support opportunities, as appropriate.

Agency Responsibilities:

- Within 30 calendar days of the initial publication of the reference architectures issued by CISA, identify resourcing and implementation gaps associated with implementing the CEM and RIF security objectives.
- Complete a logging self-assessment based on the reference architecture issued by CISA within 90 calendar days of its initial publication.

Establishment of an interagency enterprise logging working group:

Within four months of the issuance of this memorandum, the CISO Council will establish an interagency working group for cybersecurity event logging. This working group will advise CISA on any updates of the logging reference architecture. The working group will leverage existing cybersecurity regimes and industry best practices wherever feasible, so that logging and log management best practices are appropriately integrated into agency security programs.

Section IV: Requirements for FISMA Reporting to OMB and DHS

CIO, IG, and Senior Agency Official for Privacy (SAOP) metrics together provide insight into an agency's information security and privacy performance. To meet FISMA requirements, agencies report the status of their information security and privacy programs to OMB, and IGs conduct annual independent assessments of those programs. OMB and CISA collaborate with interagency partners to develop the CIO FISMA metrics, and with IG partners to develop the IG FISMA metrics to facilitate these processes. OMB also develops SAOP metrics for Federal privacy programs.

For consistency of reporting across the agency, the SAOP and CIO should coordinate on responses to the annual CIO and SAOP metrics, where there may be crossover.

Table I: Annual and Quarterly FISMA Reporting Deadlines (FY 2025)

Activities	Deadlines	Responsible Parties
• Annual CIO and SAOP Metrics • Agency Annual Report • IG Annual Report • Agency Head Letter	• October 31, 2025 (FY 2025)	All agencies
• Annual IG Metrics	• August 1, 2025 (FY 2025, Core metrics + Supplemental Metrics)	All agencies
• Quarterly CIO Metrics	• January 31, 2025 (Q1 FY 2025) • April 25, 2025 (Q2 FY 2025) • August 1, 2025 (Q3 FY 2025)	• CFO Act agencies must report on all metrics • Non-CFO Act agencies must report on all EO-related metrics[19]
• CDM-CyberScope Pre-population • FedRAMP-CyberScope Inventory Pre-population	• January 17, 2025 (Q1 FY 2025) • April 11, 2025 (Q2 FY 2025)	• CISA CyberScope, in coordination with CDM PMO and FedRAMP PMO

[19] Note that only EO metrics will be captured quarterly. Other metrics will be reported semi-annually.

	- July 18, 2025 (Q3 FY 2025) - September 30, 2025 (FY 2025)	

Section V: CIO Reporting

OMB and CISA use CIO metrics reporting to track implementation of NIST standards and cybersecurity-related initiatives, including those in support of E.O. 14028. Agencies can benefit from a review of information security governance, in particular the outcomes reflected in the "Govern" function of CSF 2.0. Governance includes cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and, the oversight of cybersecurity strategy. Through these, governance helps prioritize cybersecurity activities and is critical for incorporating cybersecurity into an organization's broader enterprise risk management strategy.

Reflecting the Administration's shift in focus 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*, Binding Operational Directive 18-02, *Securing High Value Assets*, and High Value Asset Program Supplemental Guidance 3.0, the CIO metrics are not limited to assessments and capabilities within NIST security baselines, and agency responses should reflect actual implementation levels.

OMB will identify agency programs that require additional support using CIO metrics and will utilize targeted agency engagement sessions to improve outcomes of agency information security programs and cybersecurity-mission programs.

For quarterly CIO Metrics automated through CDM, CISA will populate those values in CyberScope for agency review no later than two weeks prior to the deadline. For annual CIO Metrics automated through CDM, CISA will populate those values in CyberScope for agency review no later than four weeks prior to the deadline.

Section VI: IG Reporting

OMB, CISA, CIGIE, agency CISOs, and other stakeholders coordinate in the development of a set of metrics for use by IGs in their evaluation of the effectiveness of agency information security programs and practices. These metrics are referred to as "IG metrics." All agencies will report on IG metrics annually, through an assessment conducted by the agency IG or an independent assessor. OMB is encouraging agencies to continue their shift to a continuous assessment process for their independent assessment. To help facilitate this, OMB and CIGIE are transitioning the IG metrics process to a multi-year cycle, as described below.

OMB selected a core group of metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will continue to be evaluated in metrics on a 2-year cycle based on a calendar agreed to by CIGIE, the CISO Council, OMB, and CISA. In addition, CFO Act agency IGs should also include a summary of the data collected by CSF capability levels in the executive summary of their annual report. These changes do not in any way limit the scope of IG authority to evaluate information systems on an as-needed or ad-hoc basis.

Historically, the findings of an IG assessment were released alongside annual reporting in October, but the agency assessed may not receive funding to remediate any problems identified until two or more years after the date of the report. To help remedy this situation, starting in FY 2022, OMB shifted the due date of the IG metrics from October to July to better align the release of IG assessments with the development of the President's Budget.

Reflecting OMB's shift in emphasis away from compliance in favor of risk management, IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency. Additionally, IG audits should account for agency-specific factors such as threat analysis, risk to mission areas, technical capabilities, and complexity where appropriate, and focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls.

OMB will continue to work with CIGIE in laying the groundwork for future changes in the evaluating the current methods IGs to determine effectiveness of cybersecurity program management across the Federal Government.

Section VII: SAOP Reporting

As handling privacy issues becomes ever more important to agencies' ability to deliver on their missions, agencies must take appropriate measures to manage privacy risks and comply with privacy requirements.

Agencies are required to submit their SAOP metrics annually. In addition to those metrics, SAOPs must submit each of the following items as separate documents through CyberScope:

- The agency's privacy program plan;[20]
- 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;[21]
- The agency's privacy continuous monitoring strategy;[22]
- The Uniform Resource Locator (URL) for the agency's privacy program page,[23] as well as the URL for any other sub-agency-, component-, and/or program-specific privacy program pages;

[20] OMB Circular A-130, Appendix I § 4(c)(2), 4(e)(1).

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

[22] OMB Circular A-130, Appendix I § 4(d)(9), 4(e)(2).

[23] OMB Memorandum M-23-22, *Delivering a Digital-First Public Experience* (Sept. 22, 2023).

- 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;[24] and
- As coordinated with the agency's CIO, CISO, and other relevant officials, a description of steps the agency has taken to comply with the Creating Advanced Streamlined Electronic Services for Constituents Act of 2019 and OMB Memorandum M-21-04, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act* (Nov. 12, 2020), along with the URL on the agency's website where the required access and consent forms are posted.

As described in OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, OMB uses these reports from agencies to develop its annual FISMA report to Congress.[25]

Section VIII: Agency Head Letter for Annual Reporting Requirement to OMB

FISMA requires agency heads to be responsible for ensuring their respective agencies maintain protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of: (1) information collected or maintained by or on behalf of an agency; or (2) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

Agency heads must maintain awareness of their agency's information security programs and direct CIOs and CISOs to implement appropriate security measures and, where necessary, take remedial actions to address known vulnerabilities and threats. CIOs and CISOs need to understand adversarial capabilities and what information, information systems, and missions are attractive to threat actors.

Agency heads also are ultimately responsible for ensuring the protection of privacy interests and the responsible management of personally identifiable information within the agency. Executive Order 13719 requires each agency head to designate or re-designate an SAOP who has agency-wide responsibility and accountability for the agency's privacy program.[26]

Where there is crossover between their respective areas of responsibility, CIOs, CISOs, and SAOPs must coordinate on the contents of the agency head letter—e.g., in reporting on breaches and major incidents that are breaches, in accordance with the roles for tracking and documenting breaches outlined in OMB Memorandum M-17-12.[27]

[24] OMB Circular A-130 § 5(f)(1)(f).
[25] OMB Circular A-108 § 13 (Dec. 2016).
[26] OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016).
[27] OMB M-17-12 § VIII.

Requirement: OMB requires a signed letter from the agency head to the OMB Director and DHS Secretary as part of the annual reporting package to OMB to verify the agency head's awareness and validate the agency's FISMA report. The letter must contain the following information:[28]

A. A detailed assessment of the adequacy and effectiveness of the agency's information security policies, procedures, and practices, including details on their assessment of FY 2025 FISMA CIO metrics;
B. Details on the total number of information security incidents,[29] including a specification of the total number of breaches, reported through the CISA Incident Reporting System; and
C. A description of each major incident, if applicable, with the following details:
    - The incident description, related control failures, including attack vector, response, and remediation actions the agency has completed;
    - If the major incident was a breach, a description of the affected information[30] and the number of individuals potentially affected by the breach;[31]
    - 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.

Section IX: 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[32] their annual FISMA reports to the Chairperson and Ranking Member of the following Congressional committees:[33]

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

[28] 44 U.S.C. § 3554.
[29] 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."
[30] 44 U.S.C. § 3554(c)(1)(A)(iii)(II).
[31] 44 U.S.C. § 3554(c)(1)(A)(iii)(I).
[32] Agencies should consult with their legislative affairs office (or equivalent) for instructions on how to submit materials to Congress and the GAO.
[33] 44 U.S.C. § 3554.

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

Agency FY24 reports are due to Congress and the Government Accountability Office (GAO) **by March 1, 2025**.[34]

Section X: Incident Reporting Requirements

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

Incident Reporting

Agencies must report incidents to CISA according to current and updated requirements in the CISA Federal Incident Notification Guidelines.[35] 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 determinations for 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.

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	Details for 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.

Modernizing Incident Reporting

CISA will ensure data transmitted between agencies and CISA is in a machine-readable format. CISA will continue to provide OMB with data regarding both individual agencies' performance

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

[35] FISMA also requires agencies to notify and consult with the Federal information security incident center established in 44 U.S.C. § 3556 regarding any information security incidents. 44 U.S.C. § 3554(b)(7)(C)(ii).

in providing accurate, machine-readable data to CISA, as well as any gaps CISA has in receiving, updating, or maintaining such records.

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. This guidance does not preclude an agency from reporting an incident or breach to Congress that falls below the threshold for a major incident.

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

A major incident is EITHER:

A. An 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.[36] 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

B. 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.[37]

As with other incidents, agencies should assess each breach on a case-by-case basis to determine whether it meets the definition of a major incident. This memorandum requires a determination

[36] 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 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."

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

of major incident for any unauthorized modification of,[38] unauthorized deletion of,[39] unauthorized exfiltration of,[40] or unauthorized access to[41] the PII of 100,000 or more people; however, per the definition provided above, other factors also may lead an agency to determine that a breach is a major incident. OMB Memorandum M-17-12 details breach reporting requirements.

Reporting Major Incidents

A. Reporting to OMB and CISA

- Agencies must report to CISA and the OMB OFCIO within 1 hour of determining a major incident occurred, and should update OMB OFCIO and CISA within 1 hour of determining that an already-reported incident or breach is a major incident.[42] Agencies must reach out to both entities directly.
- Within 10 days of an agency declaring a major incident, CISA, through existing formal coordination mechanisms, will share information with agencies on the scope, relevance and potential impact of the incident as well as recommendations that enhance the posture of the federal civilian executive branch enterprise. As incident response progresses, CISA will continue to share information with agencies as it deems appropriate to include indicators of compromise and insight into necessary steps to prevent similar incidents from occurring in the future.
- Pursuant to Presidential Policy Directive-41 (PPD-41), *United States Cyber Incident Coordination*, if a cyber 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.Agencies should use the points of contact in Section X for reporting major incidents.
- When a breach is determined to be a major incident, the agency’s principal security operation center and SAOP must coordinate on tracking and documenting the major incident, in accordance with the roles outlined in OMB Memorandum M-17-12.[43]

B. Reporting to Congress and Inspectors General

[38] “Unauthorized modification” is the act or process of changing components of information and/or information systems without authorization or in excess of authorized access.
[39] “Unauthorized deletion” is the act or process of removing information from an information system without authorization or in excess of authorized access.
[40] “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.
[41] “Unauthorized access” is the act or process of gaining without permission logical or physical access to Federal information or a Federal information system, application, or other resource.
[42] 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.”
[43] OMB M-17-12 § VIII.

- An agency must notify the appropriate Congressional committees and its Office of the Inspector General (OIG) of a major incident no later than seven days after the date on which the agency determines that it has a reasonable basis to conclude that a major incident, including a breach constituting a major incident, has occurred.[44]
- 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 supplement their initial major incident report to Congress with another report no later than 30 days after the agency discovers a breach constituting a major incident.[45] 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;
    - 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.

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

[45] FISMA requires notification to be provided to the same committees identified above in the preceding footnote, plus the Committee on the Judiciary in each house of Congress. 44 U.S.C. § 3553 note.

Section XI: Contact Information and Additional Resources

Agencies will find all requirements, contact information, and appropriate points of contact for incident reporting and agency questions regarding this guidance at https://go.max.gov/e5sEF9.

The site will also include resources for agencies to leverage that may enhance and supplement internal processes and procedures for responding to incidents, such as the Cyber Incident Principal's Playbook.

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

ATTACHMENT

Appendix A:	Additional CISA Responsibilities and Agency Implications

APPENDIX A: Additional CISA Responsibilities and Agency Implications

Scanning Internet-Accessible Addresses and Systems

As required by FISMA, CISA presently provides numerous services to agencies in the interest of improving Federal information security. These responsibilities are subject to OMB oversight and applicable legal requirements.

In furtherance of its legal responsibilities and consistent with applicable law, regulation, policy, and existing Memoranda of Agreement with agencies, CISA scans internet-accessible addresses and segments of Federal civilian agency systems for vulnerabilities on an ongoing basis, as well as in response to newly discovered vulnerabilities.

No prior agency authorization is needed for one Federal agency to perform non-invasive vulnerability scanning of another Federal agency's internet-accessible systems. Federal agencies should expect that any system accessible over the public internet is being scanned for vulnerabilities by various parties at all times, and factor this into their security operations accordingly.

To ensure CISA can perform this function effectively, each Federal civilian agency shall:

- Ensure that CISA and agency security teams have points of contact on file with each other for rapid communication about any discovered vulnerabilities.
- On a semi-annual basis, provide, or continue providing, CISA a complete list of the agency's internet-accessible Federal information systems and related addressing information,[46] including static internet protocol (IP) addresses for external websites, servers, and other access points, and Domain Name Service (DNS) names for dynamically provisioned systems.[47]
- Provide CISA with notice of changes to IP ranges at least one day in advance 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

[46] CISA is not limited to the addresses and systems provided on this list when conducting its vulnerability scanning.

[47] 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).

sharing. Agencies shall provide the primary classified email address (JWICS, SIPR, or other) for the CIO Office via the CyberScope application to report on the access of these users.