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

December 6, 2021

M-22-05

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jason S. Miller
Deputy Director for Management

SUBJECT: Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements

## Purpose

This memorandum provides agencies with fiscal year (FY) 2021-2022 reporting guidance and deadlines in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).[1] This memorandum rescinds the following memoranda:

- M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*
- M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Infrastructure*

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

## Introduction

The United States Government continues to face increasingly sophisticated efforts to compromise Federal IT systems, challenging current defenses and creating an urgent need to evolve to a new security paradigm. In May 2021, the President issued Executive Order 14028, *Improving the Nation's Cybersecurity* (EO 14028), directing Federal agencies to make a series of investments in their cybersecurity defenses and begin migrating to a zero trust architecture. In support of these new initiatives, the Office of Management and Budget (OMB) is making significant changes to the current approach of FISMA oversight and metrics collection. These changes are intended to define a maturity baseline in certain high-impact capability areas, improve the quality of performance data collected at the enterprise level, and accelerate our efforts to make more informed risk-based decisions and achieve observable security outcomes.

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

OMB has identified the following tenets to guide the reform of performance management under FISMA, as reflected in this memorandum:

- **Moving to a zero trust architecture.** Agencies need to implement specific zero trust security goals by the end of Fiscal Year (FY) 2024, organized around five pillars:
    - *Identity:* Agency staff use an enterprise-wide identity to access the applications they use in their work. Phishing-resistant Multi-Factor Authentication (MFA) protects those personnel from sophisticated online attacks.
    - *Devices:* The Federal Government has a complete inventory of every device it operates and authorizes for government use, and can prevent, detect and respond to incidents on those devices.
    - *Networks:* Agencies encrypt all Domain Name System (DNS) requests and HTTP traffic within their environment, and begin executing a plan to break down their perimeters into isolated environments.
    - *Applications and Workloads:* Agencies treat all applications as internet-connected, routinely subject their applications to rigorous testing, and welcome external vulnerability reports.
    - *Data:* Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies are taking advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

- **Ground truth testing.** Traditionally, we have relied heavily on self-attestation of security control implementation, and there is a need to accelerate efforts to validate and verify those attestations. The Federal Government must rely more on methods that empirically validate security and find weaknesses, such as manual and automated penetration testing and red team exercises. The FY 2022 metrics released alongside this memorandum include a series of questions aimed at measuring the Federal Government's ability to conduct tested security.

- **Observable security outcomes.** FISMA certifications have continued to rely on compliance-based processes in which agencies and inspectors general (IGs) rely on a checklist of controls whose implementation status is used to determine the sufficiency of a system's security. This leads to an assessment of specifically scoped control-implementation successes and failures. FISMA assessments must evolve to focus on risk-based processes that will provide agencies with sufficient information to consider threat, capability, and impact. That information will enable agencies to prioritize their efforts and orient towards the greatest threats facing the nation, as well as the individual risks faced by each agency. The FY 2022 CIO metrics released alongside this memorandum include a series of questions that focus on measuring outcomes.

- **Automation.** FISMA data collection has long remained an overly manual process that often leads agencies to create complicated spreadsheets and internal processes to respond to questions. As the Federal information security apparatus matures, so should its reporting mechanisms. OMB is emphasizing automation and the use of machine-readable data to speed up reporting, reduce agency burden, and improve outcomes. This

memorandum directs development of a strategy to enable agencies to report performance and incident data in an automated and machine-readable manner.

## Section I: Additional Guidance on the President's Executive Order

Relying in part on their FISMA reporting in FY22, agencies will engage in key reporting activities throughout the next year to satisfy requirements from E.O. 14028. OMB may update required reporting metrics throughout the year as part of the effort to update and streamline reporting activities. The goal is to use existing data collection channels where possible to reduce burden while improving the quality and understanding of agency progress.

*Incident Response Playbook*

The cybersecurity vulnerability and incident response procedures currently used to identify, remediate, and recover from vulnerabilities and incidents affecting agency systems vary across agencies. Standardized response processes ensure a more coordinated and centralized cataloging of incidents and agency progress toward successful responses.

To improve incident response, Federal agencies shall:

- Use the CISA standardized playbook, including any updates, for planning and conducting cybersecurity vulnerability and incident response activities for agency information systems.
- Articulate progress and completion as required by the playbook through all phases of incident response activities.
- Use the playbook's common lexicon to express current cybersecurity status in relation to a specific incident.

Utilizing the standard incident response playbook will enhance the ability of CISA and other agencies involved in incident response and recovery to assess the risk of vulnerabilities and execute incident response activities.

## Section II: Strengthening Continuous Diagnostics and Mitigation Capabilities

*Continuous Diagnostics and Mitigation Program Overview*

The Continuous Diagnostics and Mitigation (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. CDM 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.

CISA will perform a program review of CDM and incorporate lessons learned into a strategy to continue improving the program for FY22. This strategy will articulate challenges and opportunities for improving delivery, data quality, and support for automation.

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[3] 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 cybersecurity posture and must work closely with CISA to accomplish CDM program goals within their respective agencies.

*CDM Implementation and Agency Responsibilities and Expectations*

Automated Reporting: By April 2022, CISA, in coordination with OMB and NIST, will develop a strategy to continue to evolve machine-readable data standards for cybersecurity performance and compliance data through CDM (or a successor process). This strategy will include a set of metrics (supplementing the existing CIO metrics) based on NIST Standards (e.g., NIST SP 800-53) for controls that can be reported in an automated manner, and will set forth a timeline for when these metrics will be collected automatically. These metrics should include the effectiveness of the Data Quality Management Plan (DQMP) and subsequent data exchanges.[4] OMB will use these metrics in a scorecard and will begin to grade agencies by December 2022. CISA will enable ongoing access to the data required to grade agencies on the new scorecard (through the CDM Federal dashboard or successor) to OMB and the Office of the National Cyber Director no later than December 2022.

Acquiring Capabilities: Agencies have the option to acquire continuous monitoring tools that are not procured using current or future CDM acquisition vehicles (CDM Dynamic and Evolving Federal Enterprise Network Defense [DEFEND], GSA IT Schedule 70 CDM Tools Special Item Number, etc.); however, agencies are required to provide sufficient justification prior to pursuing acquisition tools not aligned with the CDM program.[5] To do this, 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.

If an agency possesses tools and capabilities that were acquired outside of the CDM acquisition vehicles prior to the date of this memorandum, then the agency may continue to use them. In any case, agencies are required to ensure that they meet all of the CDM Federal Dashboard reporting requirements. Further, when agencies exchange data with the Federal Dashboard, they have full responsibility for responding to risks identified through the CDM program and/or the agency 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.

[3] Pub. L. No. 101-576 (1990). The current list of CFO Act agencies, as amended, appears at 31 U.S.C. § 901(b).
[4] Last year's FISMA Guidance (M-21-02) required CFO Act agencies to certify their data in accordance with the DQMP and to have the ability to exchange timely data to the Federal Dashboard by the end of FY21 Q4.
[5] 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.

Resource Allocations: When the CDM PMO procures cybersecurity tools on behalf of an agency to fulfill specific CDM requirements, the CDM PMO will cover the license and maintenance costs of the base year and the maintenance cost for the first option year. Thereafter, CFO Act agencies are responsible for funding long-term operations and maintenance (e.g., licensing costs) of their CDM-related tools and capabilities. Agencies are required to submit separate, CDM-specific line items in their annual budget documents (see OMB Circular A-11), including their congressional justification documents, as applicable. In addition, each agency should work with their OMB RMO to prepare a spending plan that details the resources (including estimated staff time) dedicated to CDM. Agencies shall, in coordination with their 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.[6]

**Section III: Requirements for FISMA Reporting to OMB and DHS**

FISMA requires agencies to report the status of their information security programs to OMB and requires IGs to 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 Senior Agency Official for Privacy (SAOP) metrics for the Federal privacy community. These three sets of metrics together provide a comprehensive picture of an agency's cybersecurity and privacy performance. For consistency of reporting across the agency, the SAOP and CIO should coordinate on responses to the annual CIO and SAOP metrics, as well as the contents of the agency head letter, where there may be crossover.

*Table I: Annual and Quarterly FISMA Reporting Deadlines (FY 2021 and FY 2022)*

| Activities | Deadlines | Responsible Parties |
|---|---|---|
| • Annual CIO and SAOP Metrics<br>• Annual Report<br>• Agency Head Letter | • October 29, 2021 (FY 21)<br>• October 31, 2022 (FY 22) | All agencies |
| • Annual IG Metrics | • October 29, 2021 (FY 21)<br>• July 30, 2022 (FY 22, Core metrics)<br>• July 30, 2023 (FY 23, Core metrics + 1/2)[7] | All agencies |
| • Quarterly CIO Metrics | • January 17, 2022 (Q1)<br>• April 15, 2022 (Q2)<br>• July 15, 2022 (Q3) | • CFO Act agencies must report on all metrics<br>• Non-CFO Act agencies must report on all EO-related metrics[8] |

[6] Non-CFO Act agencies must provide written justification to both OMB and CISA for approval.
[7] In FY23, metrics will be Core Metrics plus half of the standards and controls that will be evaluated on a two-year cycle based on a calendar agreed to by CIGIE, the CISO Council, OMB, and CISA.
[8] Note that only EO metrics will be captured quarterly. Other metrics will be reported semi-annually.

**Section IV: CIO Reporting**

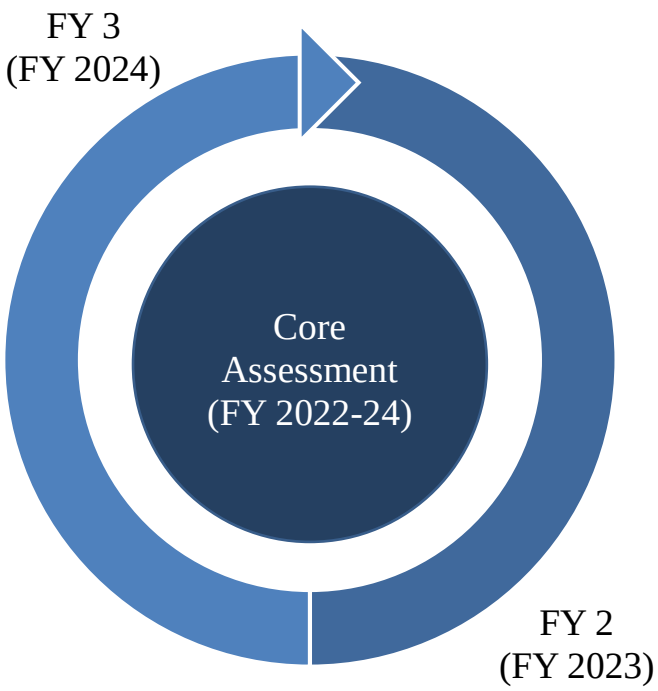
OMB and CISA use CIO metrics reporting to track implementation of the National Institute of Standards and Technology (NIST) standards, as well as other cybersecurity-related initiatives, including those in support of E O 14028.

All agencies must update their CIO metrics quarterly. 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 2.0, 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.

**Section V: IG Reporting**

OMB and CISA develop and use a set of metrics to evaluate agency implementation of policies and procedures described by NIST standards. Because these metrics are provided to the Council of the Inspectors General on Integrity and Efficiency (CIGIE), they 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 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 will select 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 be evaluated in metrics on a two-year cycle based on a calendar agreed to by CIGIE, the CISO Council, OMB, and CISA. 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.

In a typical year, the findings of an IG assessment are 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, 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. Use of this reporting timeline will begin in FY 2022, starting with the core metrics. Agencies that are unable to complete the assessment of these core metrics by the July deadline during this transitional year may request an extension by contacting ofcio@omb.eop.gov.

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, and to 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.

**Section VI: SAOP Reporting**

Given the importance of privacy, as highlighted in policies such as OMB Circular A-130, *Managing Information as a Strategic Resource*, and OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, agencies must take appropriate measures to comply with privacy requirements and manage privacy risks. SAOPs are required to report annually and must submit each of the following items as separate documents through CyberScope:

- The agency's privacy program plan;[9]
- 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;[10]
- The agency's privacy continuous monitoring strategy;[11]
- The Uniform Resource Locator (URL) for the agency's privacy program page,[12] as well as the URL for any other sub-agency-, component-, and/or program-specific privacy program pages; and
- The agency's written policy to ensure that any new collection or use of Social Security numbers (SSNs) is necessary, along with a description of any steps the agency took during the reporting period to explore alternatives to the use of SSNs as a personal identifier.[13]

**Section VII: 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 information

[9] See OMB Circular A-130, Appendix I § 4(c)(2), 4(e)(1).
[10] See OMB M-17-12.
[11] See OMB Circular A-130, Appendix I § 4(d)(9), 4(e)(2).
[12] See OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*.
[13] See OMB Circular A-130, Appendix I § 5(f)(1)(f)

collected or maintained by or on behalf of an agency; or 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.

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:[14]

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 2021 FISMA CIO metrics;
B. Details on the total number of information security incidents reported through the CISA Incident Reporting System;[15] and
C. A description of each major incident, if applicable, with the following details:
    - The incident description to include attack vector, response, and remediation actions the agency has completed;
    - Threats and threat actors, vulnerabilities, and mission and system impacts;
    - Risk assessments conducted on the information system before the date of the major incident; and
    - The status of compliance of the affected information system with security requirements at the time of the major incident.

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

**Section VIII: 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[16] their annual FISMA reports to the Chairperson and Ranking Member of the following Congressional committees:[17]

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 Governmental Affairs;

[14] 44 U.S.C. § 3554.
[15] 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).
[16] Agencies should consult with their legislative affairs office (or equivalent) for instructions on how to submit materials to Congress and the GAO.
[17] 44 U.S.C. § 3554.

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 FY21 reports are due to Congress and the Government Accountability Office (GAO) **by March 1, 2022**. Agency FY22 reports are due to Congress and the GAO **by March 1, 2023**.[18]

**Section IX: 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 Requirements.[19] 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*

[18] OMB will not review, clear, or provide a template for the reports. Agencies should submit reports directly to Congress and the GAO.
[19] 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).

An estimated 47 percent of the incidents reported in the FY 2020 Annual FISMA report were reported by agencies through the webform on the US-CERT website, rather than automatically communicated through a machine-readable data format. To ensure accurate reporting of information, agencies have historically needed to painstakingly and manually compare their incidents with US-CERT's account. By late spring of 2022, CISA, in coordination with OMB, will develop a strategy, including any technical standards, to modernize and improve the use of machine-readable incident data and indicators in a manner that communicates directly with agency SOCs and/or incident reporting systems. CISA will provide OMB real-time access to incident information no later than December 2022.

*Major Incident Definition*

FISMA directs OMB to define the term "major incident" and further instructs agencies to notify Congress in the event of a "major incident." This memorandum provides agencies with a definition and framework for assessing whether an incident is a major incident for purposes of the congressional reporting requirements under FISMA and provides specific considerations for determining the circumstances under which a breach constitutes a major incident. Additionally, this guidance does not preclude an agency from reporting an incident or breach to Congress that falls below the threshold for a major incident.

**A major incident is EITHER:**

I. Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.[20] 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.[21]

[20] 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."

[21] 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).

While agencies should assess each breach on a case-by-case basis to determine whether the breach meets the definition of a major incident, this memorandum requires a determination of major incident for any unauthorized modification of, [22] unauthorized deletion of,[23] unauthorized exfiltration of,[24] or unauthorized access to[25] the PII of 100,000 or more people. OMB Memorandum 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, in the case of a breach, the SAOP, as well. Agencies may consult with OMB and CISA to make a major incident determination.

*Reporting Major Incidents*

I. Reporting to OMB and CISA.

- Agencies must report to CISA and the OMB OFCIO within one hour of determining a major incident occurred, and should update OMB OFCIO and CISA within one hour of determining that an already-reported incident or breach is a major incident.[26]
- 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.

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 determines that it has a reasonable basis to conclude that a major incident, including a breach constituting a major incident, has occurred. [27]

[22] "Unauthorized modification" is the act or process of changing components of information and/or information systems without authorization or in excess of authorized access.
[23] "Unauthorized deletion" is the act or process of removing information from an information system without authorization or in excess of authorized access.
[24] "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.
[25] "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.
[26] 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."
[27] 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).

- 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 major incident report to Congress that is to be sent 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 has occurred with another report no later than 30 days after the agency discovers a breach constituting a major incident.[28] 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.

**Section X: Points of Contact**

- Agencies should direct questions about this memorandum and on information security program performance to OFCIO at ofcio@omb.eop.gov.
- Agencies should direct privacy-related matters to OMB's Office of Information and Regulatory Affairs (OIRA) at privacy-oira@omb.eop.gov.
- Agencies should direct questions on CyberScope reporting to CISA at FNR.FISMA@hq.dhs.gov.
- Agencies should direct questions on FISMA metrics to OMB and CISA.
- Agencies should direct questions on submission of potentially classified information to CISA at NCCIC@dhs.ic.gov with the subject line "FISMA 2022 Submission."

**ATTACHMENT**

[28] FISMA requires notification to be provided to the same committees identified above in footnote 27, plus the Committee on the Judiciary in each house of Congress. 44 U.S.C. § 3553 note.

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.

For CISA's vulnerability scanning service to be effective, it should, to the greatest extent possible, observe the same behavior in Federal systems that an adversary would be able to observe. Similarly, the origin and behavior of the scanning service should be unpredictable. To guarantee this type of emulation, CISA should initiate its vulnerability scanning service from multiple vantage points, including commercial cloud infrastructure, and from dynamically selected source addresses.

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,[29] including static internet protocol (IP) addresses for external websites, servers, and other access points, and Domain Name Service (DNS) names for dynamically provisioned systems.[30]
- Provide CISA with notice of changes to IP ranges at least one day in advance by emailing vulnerability@cisa.dhs.gov.

[29] CISA is not limited to the addresses and systems provided on this list when conducting its vulnerability scanning.
[30] 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).

**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. Agencies shall use the CyberScope application to report on the access of these users.