FY 2025
CIO FISMA Metrics

Version 1.1
December 2024

Revision History

Version	Date	Comments	Authors
1.0	12/6/2024	Initial Publication	OMB, CISA, FMSC
1.1	1/7/2025	Reverted changes to 2.4 and 2.5	OMB

Background

The Federal Information Security Modernization Act (FISMA) of 2014 (44 U.S.C. § 3554) requires the head of each federal agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Additionally, FISMA requires agency heads to report on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise.

The Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Agency (CISA) have a joint role in overseeing the information security programs of the federal enterprise. OMB issues an annual FISMA guidance document, which covers requirements for agency cybersecurity reporting, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* (FISMA Guidance). This supplemental document, the FISMA Chief Information Officer (CIO) Metrics, provides the questions agencies are required to answer under the FISMA Guidance.

The FISMA CIO Metrics provide the data needed to monitor agencies' progress towards the implementation of the Administration's priorities and best practices that strengthen federal cybersecurity. Achieving the metrics alone will not address every cyber threat, and agencies will need to implement additional defenses to effectively manage their cybersecurity risks.

In FY 2023, the FISMA Metrics Subcommittee (FMSC) was established under the Federal Chief Information Security Officer Council (CISO Council) to analyze and provide OMB with recommendations to improve current and future FISMA guidance and metrics. The FMSC provided a formalized process for federal agencies and partners to contribute to the development and maintenance of these FY 2025 FISMA CIO Metrics.

These metrics have been updated to reflect additional reporting requirements that are outlined in Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).

FISMA CIO Metrics

Enumerating the Environment

1.1 For each FIPS 199 impact level (High, Moderate, Low), what is the number of operational unclassified information systems by bureau or component (as defined by the agency) categorized at that level? (NIST SP 800-60, NIST SP 800-53 Rev. 5 RA-2)

FIPS 199 Impact Level	1.1.1	1.1.2	1.1.3	1.1.4

1.1.1 Organization-operated[1] systems

1.1.1.1 **[Source: CDM]** Number of CDM-Reported Organization-operated systems

1.1.2 Contractor-operated[2] systems

1.1.2.1 **[Source: CDM]** Number of CDM-Reported Contractor-operated systems

1.1.3 Systems (from 1.1.1 and 1.1.2) with an Authorization to Operate (ATO)[3]

1.1.3.1 **[Source: CDM]** Number of CDM-Reported Systems (from 1.1.1.1 and 1.1.2.1) with an Authorization to Operate (ATO)

1.1.3.2 **[Source: CDM]** Number of CDM-Reported Systems with an Unknown Authorization Type[4]

1.1.4 Systems (from 1.1.3) that are in ongoing authorization[5] (NIST SP 800-37 Rev. 2)

1.1.4.1 **[Source: CDM]** CDM-Reported Systems (from 1.1.3.1) that are in ongoing authorization

[1] Information systems used or operated by an agency (as defined in 44 USC § 3553 (a)(2)(B))
[2] Information systems used or operated by a contractor of an agency or other organization on behalf of the agency (as defined in 44 USC § 3553 (a)(2)(B))
[3] 'Authorization to Operate' means the official management decision given by a senior federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.
[4] Any Authorization Type that is not "Initial Authorization", "Ongoing Authorization", or "Reauthorization" is considered an "Unknown" Authorization Type in CDM. See Appendix F "Types of Authorizations" from NIST SP 800-37 Rev. 2.
[5] Systems in ongoing authorization have an active authority to operate (ATO). Systems with an active authority to operate (under 1.1.3) should be included in the total count. Systems that are enrolled in an ongoing authorization program and exceed the parameters of the program should be considered to have an active authority to operate, unless the organization's policy specifically says otherwise.

1.1.5 Number of High Value Assets (HVAs) reported to the HVA Program Management Office (PMO) via the CyberScope HVA List. Note: 1.1.5 is the sum of 1.1.5.1 and 1.1.5.2

1.1.5.1 Number of Tier 1[6]

1.1.5.2 Number of Non-Tier 1[7]

1.1.5.3 Number of HVAs pending PMO tier assignment

1.1.5.4 **[Source: CDM]** Number of CDM-Reported of HVAs[8]

1.1.6 Number of systems (from 1.1.1 and 1.1.2) that include Operational Technology (OT) and/or Internet of Things (IoT) devices.

1.1.6.1 Number of systems (from 1.1.6) that include Internet of Things devices[9].

1.1.6.2 Number of systems (from 1.1.6) that include Operational Technology[10]

1.1.6.3 Number of systems (from 1.1.6) that include both IoT and OT devices

1.1.7 Number of systems (from 1.1.6.1) that contain a device that received a waiver from meeting the requirements derived from guidance set by NIST 800- 213.

[6] Tier 1 HVAs represent systems of critical impact to both the agency and the nation. (HVA PMO)
[7] Non-Tier 1 HVAs represent systems of significant impact to both the agency and the nation. (HVA PMO)
[8] As tagged by agencies in CDM for HVA Status as "True" in the System Boundary index.
[9] As defined by NISTIR 8259
[10] As defined by NIST's Guide to Operational Technology (OT) Security, 800-82 Rev. 3

1.2 Number of hardware assets[11] operated in an unclassified environment. (Note: 1.2 is the sum of 1.2.1 through 1.2.3) (NIST SP 800-53r5 CM-8). 1.2.4 through 1.2.7 will be provided from automation activities observed and captured by CDM.

1.2.1 GFE endpoints

1.2.2 GFE networking devices

1.2.3 GFE input/output devices

1.2.4 **[Source: CDM]** Average CDM-discovered[12] GFE endpoints

1.2.5 **[Source: CDM]** Average CDM-discovered GFE networking devices

1.2.6 **[Source: CDM]** Average CDM-discovered GFE input/output devices

1.2.7 **[Source: CDM]** Average CDM-discovered "unknown" devices[13]

1.3 Percentage of total devices scanned within the timeframes below. These values are populated by CISA[14].

1.3.1 **[Source: CDM]** Every 7 days

1.3.2 **[Source: CDM]** Every 14 days

1.3.3 **[Source: CDM]** Every 30 days

1.3.4 **[Source: CDM]** More than 30 days

1.4 Total count of unsupported end-of-life/end-of-support software, and extended support software.[15]

1.4.1 Total count of unsupported Windows server licenses in use (with and without extended support).

1.4.2 Total count of unsupported Windows desktop licenses in use (with and without extended support).

---

[11] Smartphones and other mobile assets must be reported in 1.2.1 and 1.2.4; agencies should verify with CISA to determine whether these assets are currently being captured via CDM prior to providing this information.
[12] The number of discovered devices through CDM will be provided by reporting an average device count over a set number of days (e.g., 45 Day average), as contained within the Agency's CDM Dashboard. Data anomalies (e.g., "Zero" or "Null" values) will be removed to produce a consistent and stable reporting value. This data will be auto-populated by CDM 2 weeks ahead of the mandatory reporting deadline.
[13] Hardware assets not identified within the system by one of the prescribed categories (i.e., Endpoints, Networking Devices, Other input/output devices) will be tagged as an "unknown" device type until it can be accurately classified within the CDM system. Refer to Appendix A for more information on device categorization.
[14] CISA will determine this figure by providing an average over at least 6 weeks of the preceding quarter and auto populate the data no later than 2 weeks prior to the due date for agency data submissions.
[15] For 1.4 and related sub-questions, 17 occurrences of Windows XP running on agency systems would be enumerated as '17' for this calculation. This includes all software, not just Operating Systems.

1.5 Report the types of cloud services the agency is using by cloud service provider(s) and what service(s) you are receiving (e.g., mail, database, etc.) (NIST SP 800-145). Each quarter, the list of agency cloud services will be pre-populated from the FedRAMP Marketplace and agencies have the opportunity to verify and adjust their data as needed.

- **[Source: FedRAMP] Bureau:** the agency's bureau / subcomponent that authorized the cloud service (Note: agency-wide is also acceptable).
- **[Source: FedRAMP] FedRAMP Package ID:** the ID assigned by the FedRAMP Marketplace for the authorized cloud service.
- **[Source: FedRAMP] Cloud Services Provider:** the name of the third-party company or organization that delivers the cloud computing-based service (e.g., Microsoft)
- **[Source: FedRAMP] Cloud Services Offering:** the specific offering of the cloud service (Ex. Adobe Analytics).
- **[Source: FedRAMP] FedRAMP Status:** the cloud service's current authorization status with the FedRAMP Marketplace.
- **ATO Date (Agency):** the issuance date of the agency's ATO for the cloud service. This date is expected to match the "ATO Issuance Date (FedRAMP)" for that record.
- **ATO Expiration Date (Agency):** the expiration date of the agency's ATO for the cloud service. This date is expected to match the "ATO Expiration Date (FedRAMP)" for that record.
- **[Source: FedRAMP] ATO Issuance Date (FedRAMP):** the date the ATO was signed, based on the Agency ATO Letter that the FedRAMP PMO has on file.
- **[Source: FedRAMP] ATO Expiration Date (FedRAMP):** the date the ATO expires, based on the date the agency provided to the FedRAMP PMO.
- **[Source: FedRAMP] FedRAMP Authorization Date:** the date when the cloud service was authorized on the FedRAMP Marketplace.
- **[Source: FedRAMP] FedRAMP Annual Assessment Date:** the date when the FedRAMP ATO package is due for re-assessment.
- **[Source: FedRAMP] Service Type:** (Categorical) the category at which the specified cloud service is utilized for (Ex. Analytics, Collaboration).
- **[Source: FedRAMP] Service Model Type:** (Categorical) Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or Software as a Service (SaaS) (NIST SP 800-145)
- **[Source: FedRAMP] ATO on File:** (Yes or No) whether the cloud service has an ATO letter on file with the Federal Risk and Authorization Management Program (FedRAMP) PMO.
- **Decommission?:** (Yes or No) whether the pre-populated cloud service is no longer in use and should be removed from pre-population.

Multifactor Authentication and Encryption

Please answer the following questions regarding the requirements of section 3(d)(iii) of EO 14028 regarding the adoption of Multifactor Authentication (MFA) and encryption. An agency should not designate a system MFA-enabled unless it has been established that all applications included within the system boundary have been MFA-enabled.

CFO Act agencies will submit Encryption and MFA-related questions[16] to CyberScope by reporting totals for their respective component/bureau-level divisions. In situations where agencies fail to meet the targets for MFA/Encryption in Appendix B, agencies must provide system-level data for those systems that have not implemented the necessary capability to reach the target goal. The template will be available for agencies to submit data from their system-level Plan of Action and Milestones (POA&Ms) in CyberScope.

Question	Number of FISMA High Systems		Number of FISMA Moderate Systems		Number of FISMA Low Systems	
	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2
2.1 How many systems (from 1.1.1 and 1.1.2) store sensitive data?[17]						
2.1.1 How many systems (from 2.1) encrypt sensitive data at rest?						
2.2 How many systems (from 1.1.1 and 1.1.2) will only establish network connections that are encrypted in transit?[18]						

[16] Questions 1.1.1, 1.1.2, 2.1, 2.1.1, 2.2, 2.3, and 2.4

[17] Any data type with a moderate or high Confidentiality designation, per NIST SP 800-60 Vol. 2, should be considered as sensitive information.

[18] Network connections meeting this definition should be non-opportunistic, meaning that they must not fall back to unencrypted connections if an encrypted connection cannot be established.

MFA for Enterprise Identities

Question	Number of FISMA High Systems		Number of FISMA Moderate Systems		Number of FISMA Low Systems	
	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2
2.3 How many systems enforce (not optional) an MFA credential that is phishing-resistant (e.g., FIDO2, PIV) as a required authentication mechanism for enterprise identities?[19] Note: The sum of 2.3.1 + 2.3.2 cannot exceed the total number of systems provided in 2.3.						
2.3.1 How many of the systems (from 2.3) have mandatory PIV access enforced (not optional) for enterprise identities as a required authentication mechanism?						
2.3.2 How many of the systems (from 2.3) have mandatory FIDO2 enforced (not optional) for enterprise identities as a required authentication mechanism?						
2.3.3 How many of the systems with OT and/or IoT (from 1.1.6) enforce (not optional) an MFA credential that is phishing-resistant (e.g., FIDO2, PIV) as a required authentication mechanism for enterprise identities?						
2.3.4 How many systems in 1.1.6 less 2.3.3 have compensating controls[20] currently in place and operating effectively?[21]						

[19] Per M-19-17 enterprise identities "refers to the unique representation of an employee, a contractor, an enterprise user, such as a mission or business partner, a device, or a technology that a federal agency manages to achieve its mission and business objectives." It does not include public identities, as defined by M-19-17. In addition, referencing M-22-09 this metric is measuring implementation at the application layer.
[20] Per NIST SP 800-53 Rev. 5, Compensating control is defined as "The security and privacy controls employed in lieu of the controls in the baselines described in NIST Special Publication 800-53B that provide equivalent or comparable protection for a system or organization."
[21] When responding to this question, agencies may only report systems where compensating controls have been implemented, assessed, and documented as operating effectively. Controls that are not implemented or currently in remediation would not constitute effective risk mitigation. Per NIST 800-53A Rev. 5, (continued in page 10 footnote)

Question	Number of FISMA High Systems		Number of FISMA Moderate Systems		Number of FISMA Low Systems	
	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2
2.4 How many systems (from 1.1.1 and 1.1.2 less 2.3) accept MFA credentials susceptible to phishing (e.g., push notifications, OTP, or use of SMS or voice) as an acceptable authentication mechanism? Note: If a system belongs in 2.3, then it does not belong in 2.4. Sum (2.3 + 2.4) cannot exceed total number of systems (1.1.1 + 1.1.2)						
2.4.1 How many systems (from 1.1.6 less 2.3.3) accept MFA credentials susceptible to phishing (e.g., push notifications, OTP, or use of SMS or voice) as an acceptable authentication mechanism? Note: If a system belongs in 2.3.3, then it does not belong in 2.4.1. Sum (2.3.3 + 2.4.1) cannot exceed total number of systems (1.1.6)						
2.5 How many systems (from 1.1.1 and 1.1.2) allow single factor authentication such as user ID and password (e.g., MFA is optional or not available)?[22]						
2.5.1 How many systems (from 2.5) are internal facing and have mandatory PIV access enforced to get on the network where the system resides?						

control assessment includes "the testing or evaluation of the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization."

[22] Do not include systems that allow temporary, time-limited exceptions for individual users in 2.5. If a system belongs in 2.3, then it should not belong in 2.5. Sum (2.3 + 2.4 + 2.5) cannot exceed total number of systems (1.1.1 + 1.1.2). Also, note this section refers to practices in NIST SP 800-63B, section 5.1.1.2 ("Memorized Secret Verifiers"). Questions 2.7 and 2.8 refer to older practices discouraged by SP 800- 63B, and question 2.9 refer to newer practices encouraged by SP 800-63B. For reference, see https://pages.nist.gov/800-63-3/sp800-63b.html#memsecretver

Question	Number of FISMA High Systems		Number of FISMA Moderate Systems		Number of FISMA Low Systems	
	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2
2.6 How many systems in 2.4 and 2.5 have compensating controls[23] currently in place and operating effectively?[24]						
2.6.1 How many systems in 2.6 have had an auditor or assessor[25] validate the operating effectiveness of the control implementation status within the past 12 months?						
2.7 Pursuant to M-22-09, Agencies must remove password policies that require regular password rotation from all systems. How many systems (from 2.5) still require the user to change their password at periodic intervals?						
2.8 Pursuant to M-22-09, Agencies must remove password policies that require special characters from all systems. How many systems (from 2.5) require password composition rules other than length (e.g., requiring numbers, upper/lowercase and special characters?						
2.9 How many systems (from 2.5) compare user- chosen passwords against passwords known to be compromised from previous breaches and known-weak passwords (e.g., dictionary words, or the user's username)?[26]						

[23] Per NIST SP 800-53 Rev. 5, Compensating control is defined as "The security and privacy controls employed in lieu of the controls in the baselines described in NIST Special Publication 800-53B that provide equivalent or comparable protection for a system or organization."

[24] When responding to this question, agencies may only report systems where compensating controls have been implemented, assessed, and documented as operating effectively. Controls that are not implemented or currently in remediation would not constitute effective risk mitigation. Per NIST 800-53A Rev. 5, control assessment includes "the testing or evaluation of the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization."

[25] Includes Agency Inspector General assessors where applicable

[26] For an example of a federal information system performing this practice, see https://home.dotgov.gov/2018/4/17/increase-security-passwords/

MFA for Public Identities

Question	Number of FISMA High Systems		Number of FISMA Moderate Systems		Number of FISMA Low Systems	
	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2	Systems from 1.1.1	Systems from 1.1.2
2.10 How many systems (from 1.1.1 and 1.1.2) have public identities?[27]						
2.10.1 How many systems identified in question 2.10 offer phishing-resistant MFA as an option for a public identity authentication mechanism?						
2.10.2 How many systems (from 2.10 less 2.10.1) provide an option for MFA credentials susceptible to phishing (e.g., push notifications, OTP, or use of SMS or voice) as an authentication mechanism?						
2.10.3 How many of the systems identified in 2.10 allow user ID and password as the only authentication mechanism for public identities[28] (e.g., MFA is not available)?						
2.10.4 How many of the systems identified in question 2.10 accept an external federated credential service provider?[29]						

2.11 Please provide the number of systems that provide enterprise identity and access management services.

2.11.1 Please provide the number of systems subject to identity management services from a system identified under 2.11.

[27] Public Identities, per M-19-17: "Public identity refers to the unique representation of a subject that a federal agency interacts with, but does not directly manage, in order to achieve its mission and business objectives."
[28] "Do not include systems that allow temporary, time-limited exceptions for individual users in 2.10.3. If a system belongs in 2.10.1 or 2.10.2, then it should not belong in 2.10.3. Sum (2.10.1 + 2.10.2 + 2.10.3) cannot be less than or exceed the total number of systems (2.10).
[29] Per NIST SP 800-63-3, "The party that manages the subscriber's primary authentication credentials and issues assertions derived from those credentials."

Logging

Please answer the following questions related to the requirements from OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities*.

3.1 Using the model defined in OMB M-21-31, provide a self-evaluation of the maturity[30] of the agency's enterprise log management capability.

- Tier EL0 Not effective - Logging requirements focused on highest criticality are either not performed or partially performed
- Tier EL1 Basic - Logging requirements only focused on highest criticality are performed
- Tier EL2 Intermediate - Logging requirements focused on highest and intermediate criticality are performed
- Tier EL3 Advanced - Logging requirements at all criticality levels are performed

3.1.1 Of the assessment provided at the enterprise level above, provide the number of systems from 1.1.1 and 1.1.2 that are providing required data elements per M-21-31[31] for centralized access and visibility at each logging maturity level by FIPS 199 impact level.

FIPS 199 Level	**EL0**	**EL1**	**EL2**	**EL3**
High				
Moderate				
Low				

3.1.2 Please provide the number of HVAs from 1.1.5 that are providing required data elements per M-21-31[32] for centralized access and visibility:

	EL0	**EL1**	**EL2**	**EL3**
HVA				

[30] Agencies should evaluate their maturity level across their entire enterprise, considering all requirements. All requirements for a tier must be met at each agency component in order for an agency to be considered at a given tier.
[31] Agencies may have a partial implementation of systems that are meeting the requirements outlined in M-21-31, and the table in 3.1.1 is designed to capture that implementation status.
[32] Ibid. for 3.1.2.

Critical Software

Please answer the following questions related to the requirements from the initial phase of OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*. Agencies shall consult CISA's Critical Software Example List[33] for additional guidance.

4.1 As per M-21-30, "agencies must identify their critical software and adopt the required security measures for the use of that software." Provide the total number of on-premise and uniquely managed[34] software products categorized as critical software. This is a count of products rather than instances. Regardless of the number of instances deployed across an agency, the agency will count this product as one EO-Critical Software product for each uniquely managed product.

For the table below, provide the total number of on-premise and uniquely managed software products categorized as critical software for which the security measure is incorporated, the risk has been accepted for not incorporating the security measure, or the security measure is not applicable. Please note, this table only represents a subset of the required security measures outlined in Security Measures for EO-Critical Software Use.

Security Measure	Critical software incorporating security measure	Critical software for which risk of not incorporating the security measure has been accepted	Critical software where security measure is not applicable
4.1.1 Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators **(SM 1.1)**	4.1.1.a	4.1.1.b	4.1.1.c
4.1.2 Use fine-grained access control for data and resources **(SM 2.2)**	4.1.2.a	4.1.2.b	4.1.2.c
4.1.3 Protect data at rest by encrypting sensitive data **(SM 2.3)**	4.1.3.a	4.1.3.b	4.1.3.c
4.1.4 Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications **(SM 2.4)**	4.1.4.a	4.1.4.b	4.1.4.c

[33] As defined in NIST's Definition of Critical Software under Executive Order (EO) 14028.
[34] Multiple uses of the same software product, managed and deployed by different groups for different users, should be counted as discrete products by the agency. For example, if an agency uses Tableau SW on two (2) separately-managed systems, the agency should report two (2) products for the metric.

Security Measure	Critical software incorporating security measure	Critical software for which risk of not incorporating the security measure has been accepted	Critical software where security measure is not applicable
4.1.5 Back up data, exercise backup restoration, and be prepared to recover data **(SM 2.5)**	4.1.5.a	4.1.5.b	4.1.5.c
4.1.6 Use patch management practices to maintain EO-Critical Software platforms and all software deployed to those platforms **(SM 3.2)**	4.1.6.a	4.1.6.b	4.1.6.c
4.1.7 Configure logging to record the necessary information about security events involving EO-Critical Software and all software running on those platforms **(SM 4.1)**	4.1.7.a	4.1.7.b	4.1.7.c

4.2 Has the agency established a software inventory?

4.2.1 Has the agency established and maintained a software inventory for EO-Critical Software?[35]

4.3 Provide the total count of non-critical software products from the agency software inventory. (Note: 4.3 + 4.4 should equal the total count of all software products from the agency software inventory)

4.3.1 Provide the number of non-critical software products for which a software attestation is required to be collected from the software producer.[36]

[35] As required by M-21-30

[36] As required by M-22-18 and M-23-16. M-22-18 requires each federal agency to collect attestations from producers of software used by the agency if that software was developed after September 14, 2022, the effective date of M-22-18. Agencies are also required to collect attestations from producers of software developed prior to September 14, 2022, if that software is used by a federal agency and either: (1) is modified by one or more major version changes after September 14, 2022, or (2) is a hosted service that deploys continuous updates. For the purposes of M-22-18 and M-23-16, "software" includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software. Software products and components in the following categories are not in scope for M-22-18, as amended by M-23-16, and do not require a self-attestation: 1. Software developed by federal agencies; 2. Open-source software that is freely and directly obtained by a federal agency; 3. Third-party open source and proprietary components that are incorporated into the software end product used by the agency; or 4. Software that is freely obtained and publicly available.

4.3.2 Provide the number of software attestations (for non-critical software from 4.3.1) that were collected from the software producer.

4.3.3 Provide the number of extension requests (for non-critical software from 4.3.1) submitted by the agency to OMB with the associated POA&M from the software producer.[37]

4.3.4 Provide the number of waiver requests (for non-critical software from 4.3.1) submitted by the agency to OMB with the agency's risk mitigation plan.[38]

4.4 Provide the total count of critical software products from the agency software inventory. (Note: 4.3 + 4.4 should equal the total count of all software products from the agency software inventory)

4.4.1 Provide the number of critical software products for which a software attestation is required to be collected from the software producer.[39]

4.4.2 Provide the number of software attestations (for critical software from 4.4.1) that were collected from the software producer.

4.4.3 Provide the number of extension requests (for critical software from 4.4.1) that were submitted by the agency to OMB with the associated POA&M from the software producer.

4.4.4 Provide the number of waiver requests (for critical software from 4.4.1) that were submitted by the agency to OMB with the agency's risk mitigation plan.

Implementing IPv6

Please answer the following questions related to the requirements of OMB Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*. Number of GFE hardware assets (from 1.2.1-1.2.3):[40]

5.1 That only have IPv4 operational

5.2 That have both IPv4 and IPv6 operational

5.3 That only have IPv6 operational

[37] Per M-23-16, [I]f a software producer cannot attest to one or more practices identified in the attestation form… the producer of a given software application must identify the practices to which they cannot attest, document practices they have in place to mitigate associated risks, and submit a POA&M to an agency. If the agency finds the documentation satisfactory, it may continue using the software, but must concurrently seek an extension of the deadline for attestation from OMB. Extension requests submitted to OMB must include a copy of the software producer's POA&M.

[38] Per M-22-18, Agencies may request a waiver—only in the case of exceptional circumstances and for a limited duration. The waiver request must be… accompanied by a plan for mitigating any potential risks.

[39] Per M-22-18, agencies were required to "inventory all software subject to the requirements of this memorandum, with a separate inventory for "critical software."

[40] Note that 5.1 + 5.2 + 5.3 must add up to the total number GFE hardware assets from 1.2.1-1.2.3.

Workforce

Please answer the following questions regarding the agency's information security workforce program.

6.1 Fill out the following table with the agency's top 7 critical cyber workforce roles.[41] At least one role should be provided. The numbers provided may include contractors and government employees. The totals should include open billets, as well as positions that have not been created due to resource or other constraints, using the work roles defined in the NICE Framework (NIST SP 800-181 Rev. 1).

Work Role ID	Filled Positions	Vacant Positions (funded)	Emerging Need[42] (not yet created nor funded)
6.1.1.id	6.1.1.a	6.1.1.b	6.1.1.c
6.1.2.id	6.1.2.a	6.1.2.b	6.1.2.c
6.1.3.id	6.1.3.a	6.1.3.b	6.1.3.c
6.1.4.id	6.1.4.a	6.1.4.b	6.1.4.c
6.1.5.id	6.1.5.a	6.1.5.b	6.1.5.c
6.1.6.id	6.1.6.a	6.1.6.b	6.1.6.c
6.1.7.id	6.1.7.a	6.1.7.b	6.1.7.c

Ground Truth Testing

The purpose of this section is to start evaluating how agency testing procedures are currently established, conducted, and performed. Ground truth testing looks to go beyond the assumption that generic vulnerability scanning tools are sufficient for testing system security. Additionally, this section is intended to baseline how well the organization internally communicates the effectiveness of its security testing.

7.1 Please answer the following questions (Yes/No):

7.1.1 Does the agency utilize dynamic code analysis as a matter of policy and practice to test code prior to deploying it to a production environment?

7.1.2 Does the agency utilize static code analysis as a matter of policy and practice to test code prior to deploying it to a production environment?

7.1.3 Has the agency leveraged one or more public paid vulnerability reporting program (bug bounty) programs in FY25?

7.1.4 Has the agency leveraged one or more public private vulnerability reporting program (bug bounty) programs in FY25?

The following question (7.2) and sub-questions will be auto populated by CISA HVA PMO;

7.2 **[Source: CISA]** Have all HVA Tier 1 systems (from 1.1.5.1) received a CISA HVA PMO Assessment in the past 3 years? (Yes/No)

[41] As determined by agency cyber program needs (current and future).
[42] Represents the next Fiscal Year.

7.2.1 **[Source: CISA]** How many systems from 1.1.5 have received a CISA HVA PMO Tier 1 Assessment in FY25? This number should be reported as Fiscal Year to date.

7.2.1.1 **[Source: CISA]** How many HVA Tier-1 systems have outstanding major, critical, and/or high-risk findings[43] that have not been remediated within the initial 30 days of receipt of the RVA and/or SAR reports as a result of a CISA HVA PMO Tier 1 assessment? (BOD 18-02 Action 4 Part 3)

7.2.2 **[Source: CISA]** How many Systems from 1.1.5 have received Agency-led Non-Tier 1 Assessments (NT1)[44] in FY25? This number should be reported as Fiscal Year to date.

7.3 Red Team

7.3.1 Does the agency have a centralized red team[45], decentralized red teams, or no red team(s) (either staff or contracted)? (Centralized, Decentralized, No)

7.4 Threat Intelligence

7.4.1 Do agency red team and penetration testing activities incorporate active tactics, techniques and procedures (TTPs) from threat intelligence? (Yes/No)

7.4.2 Does your agency integrate threat intelligence into a Security Information and Event Management (SIEM)? (Yes/No)

7.5 Blue Team

7.5.1 Does the agency have a centralized blue team[46], decentralized blue teams, or no blue team(s) (either staff or contracted)? (Centralized, Decentralized, No)

7.6 Threat Modeling

7.6.1 How many threat model evaluations[47] were conducted Fiscal Year to Date?

---

[43] Agencies should include HVA Tier-1 systems based on outstanding major/critical weaknesses from the SAR reports and critical/high severity vulnerabilities from the RVA reports. (Source: Footnote 8 of BOD 18-02)

[44] This includes any assessments that have been conducted on HVAs per M-19-03 High Value Asset Supplemental Guidance 3.0.

[45] A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (the Blue Team) in an operational environment. Also known as Cyber Red Team. (Source: NIST Glossary)

[46] "Blue Team" refers to a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on its findings and expertise, the Blue Team provides recommendations that integrate into an overall community security solution to increase the customer's cybersecurity readiness posture. Often, a Blue Team is employed by itself or prior to a Red Team deployment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems. (Source: NIST Glossary)

[47] A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment. (Source: NIST 800-53 Rev. 5)

Smart Patching

The purpose of this section is to evaluate how well the agency is prioritizing and applying patches within the enterprise. Operations can be impacted by software patches that create unintended consequences to interoperability. However, unpatched systems can leave vulnerabilities exposed that can be exploited by adversaries. Balancing stability with an up-to-date security posture is a critical measure of whether organizations are taking vulnerability management seriously. Centralized visibility allows agencies to prioritize and rapidly mitigate threats in a changing environment.

8.1 Does your agency have a centralized[48] patch management process? (Yes/No)

8.1.1 If no, does your agency set centralized policies and standards for a patch management process? (Yes/No)

8.1.2 If yes, does the agency's centralized patch management process utilize the severity of a vulnerability (e.g., KEV, CVSS, SSVC) to prioritize patches? (Yes/No)

8.2 Does your patching prioritization process leverage significant automation?[49] (Yes/No)

8.2.1 If yes, what percentage of software assets are covered by this automation?

8.3 **[Source: CDM]** CDM-Reported mean time to remediate Known Exploited Vulnerabilities (KEVs) in days.[50]

Vulnerability Disclosure

Public vulnerability disclosure programs, where security researchers and other members of the general public can safely report security issues, are used widely across the Federal Government and many private sector industries. These programs are an invaluable accompaniment to existing internal security programs and operate as a reality check on an organization's online security posture.

9.1 What is the status of the agency's Vulnerability Disclosure Program (VDP), per OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*?

- Established, with all federal information systems in scope
- Established, with all internet-accessible systems in scope
- Established, with incomplete scope or other issues (provide clarification in text)
- Not established, in progress (provide estimated date of establishment)
- No current plans to establish a VDP (provide a detailed rationale)

[48] "Centralized" in this context means that the cybersecurity program is coordinating necessary security patches and tracking the efforts in a single centralized location. For agencies with components (e.g., bureaus, operating divisions, components, etc.) that manage patch processes independently, this would not be considered as centralized.
[49] Significant automation of patch prioritization means the calculation requires no manual input beyond initial set up and recalibration of factors.
[50] This metric should be the average time between remediation of a vulnerability and either (a) the first detection of the vulnerability; or, (b) the addition of the relevant CVE to the KEV catalog, whichever is more recent.

9.2 Number of internet-accessible[51] federal information systems (from 1.1) that are not in scope of the agency's VDP policy.

9.3 VDP Metrics (Auto-populated by CISA from BOD 20-01 Data)

VDP Metric	Value
9.3.1 **[Source: CISA]** Number of vulnerability disclosure reports	
9.3.2 **[Source: CISA]** Number of reported vulnerabilities determined to be valid (e.g., in scope and not false-positive)	
9.3.3 **[Source: CISA]** Number of currently open and valid reported vulnerabilities	
9.3.4 **[Source: CISA]** Median age (in days from receipt of the report) of currently open and valid reported vulnerabilities	
9.3.5 **[Source: CISA]** Median time to validate a submitted report	
9.3.6 **[Source: CISA]** Median time to remediate/mitigate a valid report	
9.3.7 **[Source: CISA]** Median time to initially respond to the reporter	

Resilience

10.1 Please fill in the following table regarding contingency plan activities. Data provided for the following table should be reported for systems where "covered by an annual test" means that the system has been tested within the past 365 days.

Type of Plan	Incident Response Plan	Disaster Recovery Plan	Contingency Plan
Number of High systems from (1.1.1 and 1.1.2) that have been covered by an annual test	10.1.1.a	10.1.2.a	10.1.3.a
Number of Moderate systems from (1.1.1 and 1.1.2) that have been covered by an annual test	10.1.1.b	10.1.2.b	10.1.3.b
Number of Low systems from (1.1.1 and 1.1.2) that have been covered by an annual test	10.1.1.c	10.1.2.c	10.1.3.c
Number of High systems from (1.1.1 and 1.1.2) that require this plan	10.1.1.d	10.1.2.d	10.1.3.d
Number of Moderate systems from (1.1.1 and 1.1.2) that require this plan	10.1.1.e	10.1.2.e	10.1.3.e
Number of Low systems from (1.1.1 and 1.1.2) that require this plan	10.1.1.f	10.1.2.f	10.1.3.f

[51] Internet-accessible systems include any system that is globally accessible over the public internet (i.e., has a publicly routed internet protocol (IP) address or a hostname that resolves publicly in DNS to such an address) and encompasses those systems directly.

10.2 Does the agency have an Enterprise-wide Department or Agency Office of the CIO Business Continuity Plan[52] (either stand-alone or as part of your incident response or disaster recovery plans)? (Yes/No)

10.3 Number of HVA systems (from 1.1.5) for which an Information System Contingency Plan (ISCP) has been developed to guide the process for assessment and recovery of the system following a disruption (NIST SP 800-53r5 CP-2(1), NIST SP 800-34).

10.3.1 Number of HVA systems (from 1.1.5) that have an alternate processing site[53] identified and provisioned, operate multiple redundant sites for resiliency, or can be provisioned within the organization-defined time period for resumption (NIST SP 800- 53r5 CP-7(4)).

10.3.2 Number of HVA systems (from 10.3.1) for which an alternate processing site or redundant sites have been tested in the past year.

For questions 10.4 through 10.7, please respond utilizing days, hours, minutes. If not mature enough to measure, leave blank. Please provide the following answers for the current Fiscal Year to date.

Question	Days	Hours	Minutes
10.4 Mean Time to Detect[54]			
10.5 Mean Time to Identify[55]			
10.6 Mean Time to Recover[56]			
10.7 Mean Time to Resolve[57]			

10.8 Endpoint Detection and Response (EDR)

10.8.1 For questions under 10.8.1, delineate the number of GFE (from 1.2.1):

10.8.1.1 How many GFE (from 1.2.1) are covered by at least one EDR platform in the Agency that has been coordinated and vetted through CISA's EDR initiative?

10.8.1.2 How many GFE (from 1.2.1) cannot utilize the EDR capabilities of the platforms identified in 10.8.1.1?

10.8.1.3 How many GFE (from 10.8.1.2) are covered by other on-device tools that provide centralized visibility and fit-for-purpose threat detection and response capabilities, such as Enterprise Mobility Management (EMM) and Mobile Threat Defense (MTD)?[58]

[52] As described by OMB Circular A-130.
[53] Alternate processing sites include cloud concepts such as cross region failover or availability zones
[54] The mean amount of time it takes for the organization to discover—or detect—an incident (whether through automated or manual means).
[55] The mean amount of time between when the organization receives and investigates an alert.
[56] The mean time between the start of an incident and the complete recovery back to normal operations.
[57] The mean time between the start of an incident and full remediation, including the time spent to prevent future recurrences and post incident analysis.
[58] As described by NIST SP 1800-21A: Mobile Device Security: Corporate-Owned Personally-Enabled (COPE), September 2020.

10.8.2 - Has your agency selected an enterprise endpoint detection and response (EDR) platform for the agency/department to implement as outlined in OMB Memorandum 22- 01? (Yes/No)

10.8.2.1 Please provide the number of EDR platforms deployed across the agency.[59]

10.8.3 - Referring to CISA's EDR Maturity Model[60] (required by M-22-01), please select an operational level of maturity (initial, advanced, optimal) for your agency's utilization of EDR technology(ies) in your enterprise:

> ***Initial****: Intermittent operational use, alerts are triaged manually, as well as on an ad-hoc basis.*
>
> ***Advanced****: Moderate level of expertise depending on SOC. Tool tuning, scheduled sweeps, and conducting threat hunting activities. Some automation employed to triage events and alerts. False positives are significantly reduced.*
>
> ***Optimal****: Highly tuned and integrated into daily SOC operations (security event/incident investigations) with well-practiced incident response playbooks (automated if possible), and comprehensive reporting. False positives are exceptionally rare and automation is heavily employed to minimize human interactions with the EDR solution to triage common alerts. Dynamic policies are employed to allow the EDR solution to go beyond static identification and detection of anomalous activity.*

[59] This metric should represent the total number of platforms leveraged by the agency. If two or more agency subcomponents use the same EDR solution, but they do not roll into shared visibility, each should be counted as a separate platform.

[60] See Appendix C – EDR Maturity Model from the Federal Civilian Executive Branch (FCEB) Centralized Visibility Detection and Response Concept of Operations (CONOPs)

Appendix A: Definitions

Derived credential
A credential issued based on proof of possession and control of an authenticator associated with a previously issued credential (e.g., a PIV credential), so as not to duplicate the identity proofing process. (NIST SP 800-63-3)

End-of-Life
The original equipment manufacturer will no longer market, sell, or update equipment after a certain date. This is most often due to a newer model being released by the manufacturer that replaces the older model. During the EOL phase, the manufacturer may still offer maintenance options, but at a premium price.

End-of-Support
End-of-Support is when the manufacturer stops providing technical support for a product, including bug fixes, patches, and updates. EOS is the final phase of a product's lifecycle.

Enterprise-level
The entire reporting organization, including each organizational component that has a defined mission/goal and a defined boundary, uses information systems to execute that mission, and has responsibility for managing its own risks and performance.

IPv6-Operational
The protocol is both supported, enabled and provisioned with addresses that are routable internal and external to the enterprise.

Government Furnished Equipment (GFE)
Government Furnished Equipment (GFE) is equipment that is owned and used by the government or made available to a contractor by the government (FAR Part 45).

Hardware assets
Organizations have typically divided these assets into the following categories for internal reporting. The detailed lists under each broad category are illustrative and not exhaustive. (Note: "other input/output devices" should be used to capture other kinds of specialized devices not explicitly called out.)

- Endpoints:
    - Servers (including mainframe/minicomputers/midrange computers)
    - Workstations (desktops laptops, Tablet PCs, and netbooks)
    - Smartphones and other mobile computing devices

    - Virtual machines that can be addressed[61] as if they are a separate physical machine should be counted as separate assets,[62] including dynamic and on demand virtual environments
- Networking devices[63]
    - Modems/routers/switches
    - Gateways, bridges, wireless access points
    - Firewalls
    - Intrusion detection/prevention systems
    - Network address translators (NAT devices)
    - Hybrids of these types (e.g., NAT router)
    - Load balancers
    - Encryptors/decryptors
    - VPN
    - Alarms and physical access control devices
    - PKI infrastructure[64]
    - Other nonstandard physical computing devices that connect to the network
- Other input/output devices if they appear with their own address
    - Printers/plotters/copiers/multi-function devices
    - Fax portals
    - Scanners/cameras
    - Accessible storage devices
    - VOIP phones
    - Other information security monitoring devices or tools
    - Other devices addressable on the network
- Internet of Things (IoT)
- Operational Technology (OT)

Both GFE assets and non-GFE assets are included if they meet the other criteria for inclusion listed here.[65] Note: If a non-GFE asset is allowed to connect, it is especially important that it be inventoried, authorized, and correctly configured prior to connection.

Information system(s)
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[61] Addressable" means identifiable by IP address or any other method to communicate to the network.
[62] Note that VM "devices" generally reside on hardware server(s). Assuming that both the hardware server and the VM server are addressable on the network, both kinds of devices are counted in the inventory. Agencies with questions about how to apply this principle for specific cloud providers may contact FedRAMP for further guidance: https://fedramp.gov
[63] This list is not meant to be exhaustive, as there are many types of networking devices. Note that some of these examples may overlap with IoT/OT.
[64] PKI assets should be counted as constituent assets on networks in which they reside.
[65] If a non-GFE asset connects in a limited way such that it can only send and receive presentation-layer data from a virtual machine on the network, and this data has appropriate encryption (such as a Citrix connection), it does not have to be counted.

Network
Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.[66]

Personal Identity Verification (PIV) credentials
A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation, etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable). (FIPS 201-2).

Unclassified information system(s)
Information system(s) processing, storing, or transmitting information that does not require safeguarding or dissemination controls pursuant to Executive Order 13556, *Controlled Unclassified Information*, and has not been determined to require protection against unauthorized disclosure pursuant to Executive Order 13526, *Classified National Security Information*, or any predecessor or successor Order, or the Atomic Energy Act of 1954, as amended.

Unclassified environment
A collection of interconnected components that constitute unclassified information system(s). For FISMA reporting purposes, these components are limited to endpoints, mobile assets, network devices, and input/output assets as defined under hardware assets.

[66] https://csrc.nist.gov/Glossary/?term=233#AlphaIndexDiv