FY 2023
CIO FISMA Metrics

Version 2.0

June 2023

Revision History

Version	Date	Comments	Authors
1.0	12/13/2022	Initial Publication	OMB, CISA
2.0	6/6/2023	• Updated language and references • (3) New Footnotes, (2) Removed • Further clarity on Critical Software • Minor reference updates for 2.1 and 10.3.1	OMB, CISA

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 2023 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.

These metrics have been updated to reflect some of the 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 800-53r5 RA-2)

FIPS 199 Impact Level	1.1.1	1.1.2	1.1.3	1.1.4

1.1.1 Organization operated systems

1.1.2 Contractor operated systems

1.1.3 Systems (from 1.1.1 and 1.1.2) with an Authority to Operate (ATO)

1.1.4 Systems (from 1.1.3) that are in ongoing authorization[1] (NIST SP 800-37r2)

1.1.5 Number of High Value Asset (HVA) systems reported to the BOD 18-02 data call in CyberScope. (OMB M-19-03, DHS BOD 18-02, provided by DHS HVA PMO)[2] 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

1.1.5.2 Number of Non-Tier 1

1.1.6 Number of systems (from 1.1.1 and 1.1.2) that include Operational Technology[3] devices.

1.1.7 Number of systems (from 1.1.1 and 1.1.2) that include Internet of Things platforms.[4]

1.1.7.1 Number of systems from 1.1.7 with Internet of Things devices or platforms that have received a waiver from meeting standards set by NIST 800-213.

[1] 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.
[2] Agencies no longer report their HVAs to HSIN. Agencies report this information to the BOD 18-02 data call in CyberScope, and it is automatically inserted into the CIO metric data call as a read-only value. If the agency is continuing to report this value through the BOD 18-02 data call, they will not need to provide a value for this metric.
[3] As defined by SP 800-37 Rev2
[4] As defined by NISTIR 8259

1.2. Number of hardware assets[5] 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 Average CDM discovered[6] GFE endpoints

1.2.5 Average CDM discovered GFE networking devices

1.2.6 Average CDM discovered GFE input/output devices

1.2.7 Average CDM discovered "unknown" devices

1.3. Percentage of total devices scanned within the timeframes below. These values are populated by CISA[7].

1.3.1 Every 7 days

1.3.2 Every 14 days

1.3.3 Every 30 days

1.4. Total count of unsupported end of life/end of service software, and extended support software.[8]

1.4.1 Total count of active extended support licenses.

1.4.2 Total count of unsupported Windows server licenses in use

1.4.3 Total count of unsupported Windows desktop licenses in use

[5] Smartphones and other mobile assets must be reported in 1.2.1 and 1.2.5; agencies should verify with CISA to determine whether these assets are currently being captured via CDM prior to providing this information.
[6] 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.
[7] 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.
[8] For 1.3.4 and related sub-questions, 17 occurrences of Windows XP running on agency systems would be enumerated as '17' for this calculation.

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)

Cloud Service Provider	FedRAMP Package ID	Agency ATO Date	Service Type	Service Model Type (Categorical)	ATO Letter with FedRAMP PMO (Yes or No)

- **Cloud Service Provider** – the name of the third-party company or organization that delivers the cloud computing-based service (e.g., Microsoft)
- **FedRAMP Package ID** – The ID for the service as outlined in the FedRAMP marketplace.
- **Agency ATO Date** – the date when the cloud service provider received its most recent formal ATO
- **Service Type (**Categorical) – a brief description of the purpose of the cloud service
    - Email
    - Collaboration
    - etc.
- **Service Model Type** (Categorical) – Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or Software as a Service (SaaS) (NIST SP 800-145)
- **ATO Letter with FedRAMP PMO** (Yes or No) – whether the cloud service has an ATO letter on file with the Federal Risk and Authorization Management Program (FedRAMP) PMO

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.

Note: For the FY23 Q3 reporting period, CFO Act agencies will submit Encryption and MFA-related questions[9] to CyberScope by reporting totals for their respective component/bureau-level divisions.

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?[10]						
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, where the encrypted network connection guarantees confidentiality, authenticity, and integrity?[11]						

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

[10] Any data type with a moderate Confidentiality, Integrity, or Availability designation, per NIST SP 800-60 vol 2, should be considered as sensitive information.

[11] 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?[12]						
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?						
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
2.3.3 How many systems from 1.1.2 have MFA credentialing implementation requirements in existing contract language?	N/A		N/A		N/A	

[12] 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

2.3.4 How many systems from 2.3.3 have MFA credentialing implementation requirements for FIDO2 and/or PIV in existing contract language? Note: This number cannot exceed the number provided for 2.3.3.	N/A		N/A		N/A	
2.4 How many systems (from 1.1.1 and 1.1.2 less 2.3) use MFA credentials susceptible to phishing (e.g., push notifications, OTP, or use of SMS or voice) as the primary required 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)						
2.5 How many systems (from 1.1.1 and 1.1.2) allow user ID and password as an authentication mechanism (e.g., MFA is optional or not available)?[13]						

[13] 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
2.5.1 How many of the 2.5 systems that allow user ID/password are internal facing and have mandatory PIV access enforced to get on the network where the system resides?						
2.6 How many systems in 2.4 and 2.5 have compensating controls[14] currently in place and operating effectively?[15]						
2.6.1 How many systems in 2.6 have had an external auditor or assessor 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) 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						

[14] Per, NIST SP 800-30 Rev. 1, Compensating control is defined as "A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system."

[15] When responding to 2.6, 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."

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
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)?[16]						

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?[17]						
2.10.1 How many systems identified in question 2.10 have phishing resistant MFA as an option for a public identity authentication mechanism?						
2.10.2 How many systems identified in question 2.10 provide an option for MFA credentials susceptible to phishing (e.g., push						

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

[17] 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."

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
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 (e.g., MFA is not available)?						
2.10.4 How many of the systems identified in question 2.10 trust an external federated credential service provider[18] (e.g., partner agencies, mission partners) to access systems with a credential asserting the proper xAL determined by the Digital Identity Risk Assessment (DIRA) in accordance with NIST SP 800-63-3?						

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.

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[19] of the agency's enterprise log management capability.

[18] Per NIST SP 800-63-3, "The party that manages the subscriber's primary authentication credentials and issues assertions derived from those credentials."

[19] 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.

- 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[20] 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[21] for centralized access and visibility:

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

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 list of categories of Critical Software[22] 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[23] 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.

[20] 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.
[21] Ibid. for 3.1.2.
[22] As defined in NIST's Definition of Critical Software under Executive Order (EO) 14028.
[23] If the same product is managed and deployed by different groups for different users, the agency should tabulate this as more than one count. For instance, separately managing instances of Tableau would count as two instances.

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
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[24]?

[24] As required by M-21-30

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):[25]

5.1 That only have IPv4 operational

5.2 That have both IPv4 and IPv6 operational

5.3 That only have IPv6 operational

Workforce

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

6.1 Fill out the following table. 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, for the following work roles from the NICE Framework (SP 800-181 Rev. 1).

Work Role	Filled positions	Vacant positions (funded)	Emerging Need (not yet created nor funded)
Cyber Defense Incident Responder	6.1.1.a	6.1.1.b	6.1.1.c
Secure Software Assessor	6.1.2.a	6.1.2.b	6.1.2.c
Testing and Evaluation Specialist	6.1.3.a	6.1.3.b	6.1.3.c
Vulnerability Analyst	6.1.4.a	6.1.4.b	6.1.4.c
Warnings Analyst	6.1.5.a	6.1.5.b	6.1.5.c
Security Architect (Cloud)[26]	6.1.6.a	6.1.6.b	6.1.6.c
Information Systems Security Developer	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 fill out the following tables providing the cumulative testing activities over the current fiscal year to date.

[25] 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.
[26] While the NICE Framework Security Architect definition includes all cybersecurity elements, this question is seeking expertise in cloud security.

FIPS 199 Level / Categories	High	HVA
7.1.1 Number of systems that received penetration testing using expert, system-specific analysis[27].		
7.1.2 Number of systems subject to a Red team exercise.[28]		

Type of Test	Total count of systems (from 1.1.1) that were subject to this form of testing	Total count of systems (from 1.1.2) that were subject to this form of testing	Total count of tests performed.
7.1.3 Dynamic code analysis[29]			
7.1.4 Static code analysis[30]			N/A
7.1.5 Public paid vulnerability reporting program (bug bounty)			
7.1.6 Private paid vulnerability reporting program (bug bounty)			

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

7.2 Have all HVA Tier 1 systems received a CISA Assessment in the past 3 years? (Y/N)

7.2.1 How many systems from 1.1.5 have received CISA Tier 1 Assessment in FY23? This number should be reported as Fiscal Year to date.

7.2.2 How many Systems from 1.1.5 have received Agency Non-Tier 1 Assessments (NT1)[31] in FY23? This number should be reported as Fiscal Year to date.

[27] See NIST SP 800-115 under Penetration Testing
[28] See NIST SP 1800-21B under Red Team Exercise
[29] See NIST SP 800-204C.
[30] Ibid.
[31] This includes any assessments that have been conducted on HVAs per M-19-03 High Value Asset Supplemental Guidance 3.0.

7.3 Red Team[32]

Please fill out the following for red team exercises:

7.3.1 Does the agency have a centralized red team, decentralized red teams, or no red team(s)? (centralized, decentralized, no)

7.3.2 In the past year, how many of the agency's cloud services (from 1.5) have performed a red team exercise on themselves?

7.3.2.1 How many of these cloud services (from 7.3.2) are required by contract to tell the agency if they have performed a red team exercise in the past year?

7.3.2.2 Of those cloud services (7.3.2.1), how many are required by contract to share full detailed[33] results with the agency?

7.3.2.3 How many of the agency's cloud service providers who are not contractually required to report red team exercise results did report those results to the agency?

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? (Y/N)

7.4.2 Does your agency have a Governance, Risk, and Compliance (GRC) tool?

7.4.2.1 If yes, does your agency's Governance Risk and Compliance (GRC) tool incorporate technical indicators from threat intelligence into its processes in an automated manner? (yes, no)

7.4.2.2 If yes, does your agency's GRC tool have the ability to consume Open Security Controls Assessment Language (OSCAL)? (yes/no)

7.4.3 Does your agency integrate threat intelligence into a SIEM? (yes/no)

7.4.4 Do your CIO and CISO have TS/SCI clearances? (yes/no)

7.4.4.1 Do your CIO and CISO with TS/SCI clearances have access to a secure terminal? (on-site, external agency, no access)

[32] 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)

[33] Full details mean that the agency may request any and all technical details of a given security assessment. Partial details would be considered reports that exclude details due to unique contractual relationships (e.g., certain information is subject to intellectual property protections or implied limitations that prevent full disclosure of operations).

7.5 Blue Team[34]

7.5.1 Does the agency have a centralized blue team, decentralized blue teams, or no blue team(s)? (centralized, decentralized, no)

7.6 Threat Modeling

7.6.1 How many threat model exercises[35] were conducted in the last reporting period?

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[36] 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?[37] (yes/no)

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

8.3 Has the agency achieved the capabilities to, and consistently met, the actions required as of April 3, 2023, under Binding Operational Directive 23-01?

8.4 Mean time to remediation of Known Exploited Vulnerabilities (KEVs) in days[38]

---

[34] "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)

[35] 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)

[36] "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.

[37] Significant automation of patch prioritization means the calculation requires no manual input beyond initial set up and recalibration of factors.

[38] 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.

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)

9.2 Number of internet-accessible[39] 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 Number of vulnerability disclosure reports	
9.3.2 Number of reported vulnerabilities determined to be valid (e.g., in scope and not false-positive)	
9.3.3 Number of currently open and valid reported vulnerabilities	
9.3.4 Median age (in days from receipt of the report) of currently open and valid reported vulnerabilities	
9.3.5 Median time to validate a submitted report	
9.3.6 Median time to remediate/mitigate a valid report	
9.3.7 Median time to initially respond to the reporter	

Resilience

10.1 Please fill in the following table regarding contingency plan activities.

Type of Plan	Number of systems (from 1.1) that have been covered by an annual test of that plan
Incident response plan	10.1.1
Disaster recovery plan	10.1.2

10.2 Does the agency have an Enterprise-wide Department or Agency Office of the CIO Business Continuity Plan (either stand-alone or as part of your incident response or disaster recovery plans) (Y/N)

[39] 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.

10.3 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 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 10.6, 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[40]			
10.5 Mean Time To Identify[41]			
10.6 Mean Time To Recover[42]			
10.7 Mean Time To Resolve[43]			

10.8 Endpoint Detection and Response (EDR)

10.8.1 - Number of GFE Endpoints (from 1.2.1) Covered By:

10.8.1.1 - At least one EDR platform in the Agency

10.8.1.2 - A mobile threat defense[44] (MTD) or other EDR-equivalent solution for non-conforming devices

10.8.1.3 – The enterprise EDR platform identified by the Agency in question 10.8.2 (if no enterprise EDR platform is selected, this is 0)

10.8.2 - Yes/No - 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?

10.8.2.1 Please provide the number of EDR platforms deployed across the agency.[45]

[40] The mean amount of time it takes for the organization to discover—or detect—an incident (whether through automated or manual means).
[41] The mean amount of time between when the organization receives and investigates an alert.
[42] The mean time between the start of an incident and the complete recovery back to normal operations.
[43] The mean time between the start of an incident and full remediation, including the time spent ensuring the failure will not re-occur and post-incident analysis.
[44] As described by NIST Special Publication 1800-21A: Mobile Device Security: Corporate-Owned Personally-Enabled (COPE), September 2020.
[45] 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.

10.8.3 - Referring to CISA's EDR Maturity Model (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:

Guidance:

Initial *Maturity: Intermittent operational use, alerts are triaged manually, as well as on an ad-hoc basis.*

Advanced *Maturity: 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 *Maturity: 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.*

Appendix A: Definitions

Contractor-operated system
A Federal information system that is used or operated by a contractor of an executive agency, or by another organization on behalf of an executive agency.

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 Service

End of Service or end of support is when the manufacturer quits selling a product and, in most cases no longer provides maintenance services or updates after a certain date. 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[46] as if they are a separate physical machine should be counted as separate assets,[47] including dynamic and on demand virtual environments
- Networking devices[48]
    - 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[49]
    - Other nonstandard physical computing devices that connect to the network
- Other input/output devices if they appear with their own address
    - Industrial control system
    - Printers/plotters/copiers/multi-function devices
    - Fax portals
    - Scanners/cameras
    - Accessible storage devices
    - VOIP phones
    - Other information security monitoring devices or tools
    - Internet of Things (IOT) devices
    - Other devices addressable on the network

Both GFE assets and non-GFE assets are included if they meet the other criteria for inclusion listed here.[50] 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.

Network
Information system(s) implemented with a collection of interconnected components. Such

[46] "Addressable" means identifiable by IP address or any other method to communicate to the network.
[47] 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
[48] This list is not meant to be exhaustive, as there are many types of networking devices.
[49] PKI assets should be counted as constituent assets on networks in which they reside.
[50] 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.

components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.[51]

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.

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