FY 2022
CIO FISMA Metrics

Version 1

December 2021

Revision History

Version	Date	Comments
1.0	8/2021	Draft release for agency comment

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 2021-2022 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)

Bureau or component	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 (NIST SP 800-37r2)

1.1.5 Number of High Value Asset (HVA) systems reported to Homeland Security Information Network (HSIN) this quarter. (OMB M-19-03, DHS BOD 18-02, provided by DHS HVA PMO)[1]

1.2. Number of hardware assets 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)

1.2.1 GFE endpoints

1.2.2 GFE networking devices

1.2.3 GFE input/output devices

1.3. 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	Cloud Service Offering	Agency ATO Date	Bureau or Component	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)

[1] 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.

- **Agency ATO Date** – the date when the cloud service provider received its most recent formal ATO
- **Bureau or Component** – the name of the bureau or component (as defined by the agency) that manages the cloud service
- **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.

Question	Response
2.1 How many systems (from 1.1.1 and 1.1.2) 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?[2]	
2.3 How many of the systems (from 1.1.1 and 1.1.2) have mandatory PIV access enforced (not optional) for internal users as a required authentication mechanism?	
2.4 Of the systems that do not enforce PIV authentication for internal users (total number of systems from 1.1.1 and 1.1.2 less 2.3), how many enforce (not optional) an MFA credential that is verifier impersonation-resistant (e.g. mutual TLS, or Web Authentication) as a required authentication mechanism?	
2.5 How many systems (from 1.1.1 and 1.1.2 less 2.3 and 2.4) use MFA credentials susceptible to impersonation (e.g. push notifications, OTP, or use of SMS or voice) as the primary required authentication mechanism?	
2.6 How many systems (from 1.1.1 and 1.1.2) allow user ID and password as the only authentication mechanism (e.g., MFA is optional or not available)?[3]	

[2] 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.
[3] This section refers to practices in NIST SP 800-63B, section 5.1.1.2 ("Memorized Secret Verifiers"). Questions 2.7 and 2.7.1 refer to older practices discouraged by SP 800-63B, and questions 2.8 and 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	Response
2.6.1 How many systems from 2.6 are not internet-facing but have mandatory PIV access enforced (not optional) for internal users as a required authentication mechanism to gain access to the system through a network connection?	
2.7 How many systems (from 2.6) require the user to change their password at periodic intervals, whether or not the credential is known to be compromised?	
2.8 How many systems (from 2.6) require password composition rules other than length (e.g., requiring numbers, upper/lowercase and special characters; restricting dictionary words and the user's username)?	
2.9 How many systems (from 2.6) 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)?[4]	
2.10 How many systems (from 1.1.1 and 1.1.2) have external (non-department/agency) user accounts?	
2.10.1 How many systems identified in question 2.10 have mandatory PIV or other xAL3 access enforced (not optional) for external users as a required authentication mechanism?	
2.10.2 Of the systems that do not enforce PIV or xAL3 authentication for external users (2.10 less 2.10.1), how many enforce (not optional) an MFA credential that is verifier impersonation-resistant (e.g. mutual TLS, or Web Authentication) as a required authentication mechanism?	
2.10.3 Of the systems that do not enforce PIV or xAL3 authentication for external users (2.10 less 2.10.1 and 2.10.2), how many enforce (not optional) MFA for external user accounts with a credential that is not verifier impersonation-resistant (e.g., push notifications, OTP, or use of SMS or voice) as a required authentication mechanism?	
2.10.4 How many of the systems identified in 2.10 allow user ID and password as the only authentication mechanism (e.g., MFA is optional or not available)?	
2.10.5 How many of the systems identified in question 2.10 trust an external federated Identity Provider (IDP) (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?	

2.12 Per EO 14028, section 3(d)(iii), agencies are required to fully adopt MFA and encryption for **encrypting data at rest**. If the agency has not fulfilled these requirements, what is the primary barrier for the agency to meeting these requirements? Select one of the following categories and optionally provide clarifying text.

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

- These requirements are already fulfilled
- Budget – the agency lacks sufficient monetary resources to complete
- Technology – the technology to implement on some systems does not exist
- Workforce – the agency does not have available employees or contractors with skillsets that would allow for implementation
- Other (please specify in text)

2.13 Per EO 14028, section 3(d)(iii), agencies are required to fully adopt MFA and encryption for **encrypting connections in transit**. If the agency has not fulfilled these requirements, what is the primary barrier for the agency to meeting these requirements? Select one of the following categories and optionally provide clarifying text.

- These requirements are already fulfilled
- Budget – the agency lacks sufficient monetary resources to complete
- Technology – the technology to implement on some systems does not exist
- Workforce – the agency does not have available employees or contractors with skillsets that would allow for implementation
- Other (please specify in text)

2.14 Per EO 14028, section 3(d)(iii), agencies are required to fully adopt MFA and encryption for **multifactor authentication**. If the agency has not fulfilled these requirements, what is the primary barrier for the agency to meeting these requirements? Select one of the following categories and optionally provide clarifying text.

- These requirements are already fulfilled
- Budget – the agency lacks sufficient monetary resources to complete
- Technology – the technology to implement on some systems does not exist
- Workforce – the agency does not have available employees or contractors with skillsets that would allow for implementation
- Other (please specify in text)

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

(Optional, except during annual FY 2022 collection; will be required quarterly in FY 2023)

- Tier IL0 Not effective - Logging requirements focused on highest criticality are either not performed or partially performed
- Tier IL1 Basic - Logging requirements only focused on highest criticality are performed
- Tier IL2 Intermediate - Logging requirements focused on highest and intermediate criticality are performed
- Tier IL3 Advanced - Logging requirements at all criticality levels are performed

3.1.1 Of the assessment provided at the enterprise level above, provide a self-evaluation of the agency's component/bureau-level self-evaluation of the agency's incident log management maturity in the table below. For agencies where components/bureaus independently manage the collection of logs, which are then provided to the enterprise log management capability, please evaluate the maturity of each component/bureau's log management using the maturity model defined in OMB M-21-31.

Component/Bureau	**Incident Log Management Maturity Rating Tier (IL0, IL1, IL2, IL3)**

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*.

4.0 Number of instances[6] of on-premise critical software, defined in Definition of Critical Software under Executive Order (EO) 14028, at the agency.

[5] 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.

[6] Each distinctly maintained and managed deployment of a certain configuration, package, release, and/or patch level of a software is a separate instance. Specific user instantiation (e.g., software installed on a user's laptop) shouldn't be counted; rather, the version installed would be one instance of the software license. For example, if the agency has both Tableau 10.2.1 legacy and Tableau 11.2, then

Fill out the table below for each of the following security measures outlined in Appendix A of OMB M-21-30, indicating the number of instances of on-premise critical software (from 4.0) for which the security measure is incorporated, the risk of not incorporating the security measure has been accepted, or the security measure is not applicable.

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
SM 1.1	4.1.1a	4.1.1b	4.1.1c
SM 2.2	4.1.2a	4.1.2b	4.1.2c
SM 2.3	4.1.3a	4.1.3b	4.1.3c
SM 2.4	4.1.4a	4.1.4b	4.1.4c
SM 2.5	4.1.5a	4.1.5b	4.1.5c
SM 3.2	4.1.6a	4.1.6b	4.1.6c
SM 4.1	4.1.7a	4.1.7b	4.1.7c

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)*.

5.1 Number of GFE hardware assets (from 1.2.1-1.2.3) that are fully IPv6-enabled.[7]

Workforce

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

6.1 Fill out the following table, taking into consideration the level of risk at the agency. 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	Number of additional FTEs of this work role necessary to meet information security program needs
Forensics Analyst	6.1.1
Incident Responder	6.1.2
Secure Software Assessor	6.1.3
System Testing and Evaluation Specialist	6.1.4
Vulnerability Assessment Analyst	6.1.5
Threat/Warning Analyst	6.1.6

that is two separate instances, but if a laptop has a copy of Tableau 9.1, that copy does not count as a separate instance.

[7] An asset is "fully IPv6-enabled" if the IPv6 protocol is fully supported and is operationally enabled for native use (i.e., not tunneled over or translated to IPv4) for all network functions.

Exploitation Analyst	6.1.7

6.2 List the top[8] three work roles[9] from the NICE Framework (excluding those work roles listed in 6.1) necessary to meet the agency's information security program needs. (Optional)

6.3 Briefly describe the most significant barrier to the agency in meeting its information security workforce needs. Select one of the following categories and optionally provide clarifying text.

- Budget – the agency lacks the sufficient monetary resources to sufficiently staff.
- Pay flexibility – ability to pay employees beyond base levels to secure and retain top talent.
- Lack of expertise – skillsets of greatest need have limited talent pool.
- Clearances – ability to hire individuals that meet clearance requirements in a timely manner.
- Other (please specify in text).

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 table for testing activities for the last reporting period[10]

Type of Test	Total count of systems (from 1.1.1 and 1.1.2) that received this form of testing	Total count of tests performed
7.1.1 Penetration test (using automated tools only)		
7.1.2 Penetration test (using manual, expert, system-specific analysis[11])		
7.1.3 Red team exercise[12]		
7.1.4 Static and dynamic code analysis		
7.1.5 Public paid vulnerability reporting program (bug bounty)		

[8] Based on criteria determined by the agency.
[9] See list here for ease of reference: https://niccs.cisa.gov/about-niccs/workforce-framework-cybersecurity-nice-framework-work-roles
[10] For January (Q1), report the past year beginning at the start of FY21 Q2 (January 15, 2021).
[11] This refers to penetration testing that is typically more time-intensive, specialized, and application-specific. For example, scanning a web form for common vulnerabilities would not meet this definition. Activities that would more likely meet this definition could include attempting to submit creatively invalid data while taking into account the specific kinds of data requested by the form, or evaluating whether form-specific client-side validation logic is also consistently validated on the server.
[12] https://csrc.nist.gov/glossary/term/red_team_exercise

7.1.6 Private paid vulnerability reporting program (bug bounty)		
7.1.7 CISA Risk and Vulnerability Assessment (RVA)		
7.1.8 CISA Validated Architecture Design Review (VADR)		

7.2 Penetration Testing

For the following questions, provide responses for the last reporting period:[13]

7.2.1 How many government FTEs directly performed penetration testing on agency information systems for your organization?

7.2.2 How many contractor FTEs directly performed penetration testing on agency information systems?

7.2.3 How many penetration tests (from 7.1) were conducted via an external contract?

7.2.4 What was the cost (in millions of dollars) of penetration tests (from 7.1) conducted?

7.2.5 What tools were used to perform penetration tests?

7.2.6 What tools were used to perform static and dynamic code analysis?

7.2.7 What tools were used to support public and private vulnerability disclosure programs and bug bounties?

Product Name	Vendor	Version	Enterprise-Wide?

7.3 Red Team[14]

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 How many exercises discovered new vulnerabilities (inclusive of business process vulnerabilities) that were not already discovered and tracked in existing vulnerability tracking or by audits performed by a third party?

[13] For January (Q1), report the past year beginning at the start of FY21 Q2 (January 15, 2021); otherwise, provide responses for the current quarter.

[14] 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)

7.3.3 In the past year, how many of the agency's cloud services (from 1.3) have performed a red team exercise on themselves?

7.3.3.1 How many of these cloud services (from 7.3.3) are required by contract to tell the agency if they have performed a red team exercise in the past year?

7.3.3.2 Of those cloud services (7.3.3.1), how many are required by contract to share full detailed[15] results with the agency?

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

7.4 Threat Intelligence

7.4.1 Please provide a description of how your red team(s) utilize threat intelligence in their exercise procedures. If the agency does not have any red teams, please provide an explanation how your organization utilizes threat intelligence in system assessment procedures.

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)?

7.4.2.3 If no, please provide an explanation of how your organization is storing, collecting, and processing technical indicators across your enterprise.

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

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

[15] 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[16]

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

7.5.2 In the last reporting period,[17] what was the mean reaction and escalation response time in the event the red team exercise activities were discovered? (value and time unit, not mature enough to measure, no blue team)

7.6 Threat Modeling

7.6.1 How many threat model exercises[18] 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.

8.1 Does your agency have a centralized[19] patch management process? (yes/no)

8.1.1 If no, does your agency set standards for a patch management process? (yes/no)

8.1.2 Does the agency patching management process utilize the severity of a vulnerability (e.g. CVSS) to prioritize patches? (yes/no)

8.1.3 Does your agency use methods other than CVSS to analyze the severity of vulnerabilities? (yes/no – if yes, state which methods)

8.1.4 Describe the extent to which the agency applies threat intelligence in its patching process.

---

[16] "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)

[17] For January (Q1), report past year (January 1, 2021 to December 31, 2021); otherwise, provide responses for the previous quarter

[18] 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)

[19] "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.

8.2 Does your patching prioritization process leverage significant automation?[20] (yes/no)

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

8.3 What elements of the Systems Development Life Cycle (SDLC) contribute to significantly reducing the timeliness of your patching processes (e.g., patches are bundled with other change requests and subsequently require lengthy review processes)?

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 Provide a copy of the latest VDP process flow or standard operating procedure (SOP)

9.3 Number of triaged vulnerability reports received through VDP (since last reporting period)[21]

9.4 Number of systems (from 1.1) on which vulnerabilities reported through VDP were found

9.5 Number of Federal information systems (from 1.1) that are outside current scope of VDP **and** internet-accessible[22]

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 a test of that plan
Incident response plan	10.1.1
Disaster recovery plan	10.1.2
Business continuity plan	10.1.3
Business Impact analysis	10.1.4

[20] Patch prioritization calculation requires no manual input beyond initial set up and recalibration of factors

[21] For January (Q1), report past year (January 1, 2021 to December 31, 2021).

[22] 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 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)

> **10.2.1** 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))
>
> **10.2.2** Number of HVA systems (from 9.4) for which alternate processing site or redundant sites have been tested in the past year

10.3 Mean time to incident first response[23] (value and time unit, or not mature enough to measure)

10.4 Mean time to incident triage[24] (value and time unit, or not mature enough to measure)

10.5 Mean time to incident resolution[25] (value and time unit, or not mature enough to measure)

Please answer the following questions related to the Incident Response Playbook required by EO 14028 and OMB M-22-XX, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*.

10.6 Has the agency evaluated the incident response playbook against its current incident response procedures? (yes/no)

> **10.6.1** If yes, when was this review completed?
>
> **10.6.2**. If yes, did the agency identify changes necessary to elevate incident response procedures to meet or exceed what is outlined in the incident response playbook? (yes/no/already exceeded)
>
> **10.6.3** If yes, what is the date when incident response procedures were updated as a result of this review?
>
> **10.6.4** Does the agency's communications strategy include activating channels (chat rooms, phone bridges, and out-of-band email) for coordination of support by agency personnel? (yes/no)
>
> > **10.6.4.1** Does the agency's communications strategy include activating channels (chat rooms, phone bridges, and out-of-band email) for coordinating with agency leadership?

[23] The elapsed time from when the report is submitted to the first public activity on a report. The first public activity includes adding a public comment, changing the report state, or changing the report severity.
[24] The elapsed time from when a report is submitted to when a report is changed to a triaged state. A report can skip the triaged state and move directly to a closed state (e.g., resolved).
[25] The elapsed time from when a report is submitted to when a report is closed.

10.6.5 Has the agency determined a process for sharing incident details with CISA, including establishing secure file share for sending data, identifying cleared personnel to receive classified CTI, and using a secure chat platform for information exchange? (yes/no)

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.[26]

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-Enabled asset
An asset where the IPv6 protocol is fully supported and is operationally enabled for native use (i.e., not tunneled over or translated to IPv4) for all network functions.

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:[27]
  - Servers (including mainframe/minicomputers/midrange computers)
  - Workstations (desktops laptops, Tablet PCs, and net-books)
  - Virtual machines that can be addressed[28] as if they are a separate physical machine should be counted as separate assets,[29] including dynamic and on demand virtual environments
- Mobile Devices:
  - Smartphone
  - Tablets
  - Pagers
- Networking devices[30]
  - Modems/routers/switches
  - Gateways, bridges, wireless access points
  - Firewalls
  - Intrusion detection/prevention systems

[26] See 44 USC 3554(a)(1)(A); NIST SP 800-171.
[27] See 44 USC 3554(a)(1)(A); NIST SP 800-171.
[28] "Addressable" means identifiable by IP address or any other method to communicate to the network.
[29] 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
[30] This list is not meant to be exhaustive, as there are many types of networking devices.

- 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[31]
- 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
- 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.[32] 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 components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.[33]

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

[31] PKI assets should be counted as constituent assets on networks in which they reside.
[32] 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.
[33] https://csrc.nist.gov/Glossary/?term=233#AlphaIndexDiv

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.