

FY 2021 CIO FISMA Metrics

Version 1
November 2020

This page is intentionally left blank

Revision History

| Version | Date | Comments | Authors | Sec/Page |
|---------|---------|---------------------|----------|----------|
| 1.0 | 11/2020 | Initial Publication | OMB/CISA | All |

Table of Contents

GENERAL INSTRUCTIONS..... 2

1 IDENTIFY..... 5

2 PROTECT 8

3 DETECT 12

4 RESPOND..... 14

5 RECOVER..... 15

APPENDIX A: SUMMARY OF FISMA CAP GOAL TARGETS & METHODOLOGY 16

APPENDIX B: DEFINITIONS..... 17

GENERAL INSTRUCTIONS

Background

The Federal Information Security Modernization Act (FISMA) of 2014 ([PL 113-283, 44 USC 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 Security 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, OMB [M-21-02, Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements](#) (FISMA Guidance).

The FISMA Chief Information Officer (CIO) metrics focus on assessing agencies' progress toward achieving outcomes that strengthen Federal cybersecurity. In particular, the FISMA metrics assess agency progress by:

1. Ensuring that agencies implement the Administration's priorities and best practices;
2. Providing the Office of Management and Budget (OMB) with the performance data to monitor agencies' progress toward implementing the Administration's priorities.

Achieving these outcomes may not address every cyber threat, and agencies may have to implement additional controls, or pursue other initiatives to overcome their cybersecurity risks.

How is this data used?

- **Annual FISMA reporting** – each year OMB releases a report to the public regarding the state of Federal cybersecurity, including recommended actions to congress and the Federal agencies, which are informed by agency responses. CIO metrics help agencies and OMB to fulfill congressional reporting requirements. Additional information on agency reporting requirements can be found in annual FISMA Guidance.
- **Cross Agency Priority (CAP) Goal reporting** – the [President's Management Agenda \(PMA\)](#) lays out a long-term vision for modernizing the Federal Government, and is comprised of a series of CAP goals which publicly track progress on achieving a series of targets and milestones. One of these CAP Goals is the [Modernizing IT for Productivity and Security Goal](#), which identifies ten priority security capability areas for the Federal agencies to meet. Details for these metrics and associated targets can be found in Appendix A below. These metrics make up a portion of the FISMA score of the [FITARA scorecard](#).
- **Risk Management Assessments (RMA)** – Section 1(c)(ii) of the [Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure](#), released May 11, 2017, directed each agency to provide a risk management report to OMB and DHS. Responses to the CIO metrics are used to

construct ratings for the RMA, which is a diagnostic tool which provides a clear framework of the administration's cybersecurity priorities that enables OMB, agency CIOs, Chief Information Security Officers (CISOs), and their leadership to use a common language to drive discussions on how best to improve cybersecurity posture. These assessments are now required to be conducted regularly as found in annual FISMA Guidance.

- **Program implementation** – in addition to their use in performance evaluation, some questions are utilized by a Program Management Office (PMO) to help fulfill their mission objectives, for example information on cloud services is periodically shared with the General Services Administration's Federal Risk and Authorization Management Program (FedRAMP) to identify services which may not be FedRAMP approved, and the CyberStat program considers agency responses when determining topics to focus on during their reviews.
- **Policy analysis** – OMB and CISA periodically issue cybersecurity related policy memoranda and Binding Operational Directives (BODs), respectively, which provide guidance on a topic area or require agencies to complete specific actions. OMB and CISA utilize responses to FISMA metrics when considering policy areas to address or update, and in order to track progress on and evaluate the success of those policies. FISMA metrics will often change as a result of a new or updated policy.
- **Exploratory measures** – select metrics are not actively being used to evaluate agency cybersecurity posture, but may be used to provide a baseline for future performance measures.
- **Budgeting** – OMB regularly collects data on agencies cybersecurity spending and budgeting as part of the submission of the [President's Budget](#). When considering the need for additional cybersecurity funding for agencies, OMB takes into consideration performance in the areas of the RMA and CAP Goals.

Structure

Since FY 2016, OMB and the CISA have organized the CIO FISMA metrics around the National Institute of Standards and Technology's (NIST) [Framework for Improving Critical Infrastructure Cybersecurity](#) (Cybersecurity Framework). The FISMA metrics leverage the Cybersecurity Framework as a standard for managing and reducing cybersecurity risks, and they are organized around the framework's five functions: Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework, when used in conjunction with [NIST's 800-37 Rev 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 800-39, Managing Information Security Risk: Organization, Mission, and Information System View](#) and associated standards, guidelines, and best practices provides agencies with a comprehensive structure for making more informed, risk-based decisions and managing cybersecurity risks across their enterprise. Per annual FISMA Guidance and following the Administration's shift from compliance to risk management, CIO Metrics are not limited to capabilities within NIST security baselines, and agency responses should reflect actual implementation levels. Additionally, OMB [M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program](#) provides guidance to agencies on their High Value Asset (HVA) programs, and OMB [M-19-17, Enabling Mission Delivery](#)

[*through Improved Identity, Credential, and Access Management*](#) provides guidance to agencies on their Identity, Credential, and Access Management (ICAM) programs.

Expected Levels of Performance

Agencies should view the target levels for FISMA metrics as the minimum threshold for securing their information technology enterprise, rather than a cybersecurity compliance checklist. In other words, reaching a performance target for a particular metric means that an agency has taken meaningful steps toward securing its enterprise, but still has to undertake considerable work to manage risks and combat ever-changing threats.

The 24 Chief Financial Officer (CFO) Act agencies must report on the status of all metrics on a quarterly basis, at a minimum, in accordance with the guidance established in FISMA Guidance. All non-CFO Act Agencies (i.e., small and independent agencies) must report on the status of all metrics on a semi-annual basis, at a minimum, in accordance with that same guidance. All agencies should provide explanatory language for any metric that does not meet established CAP Goal targets ([Appendix A](#)) or RMA capability targets. OMB will also provide guidance to agencies in the event that OMB requires agencies to report on their performance on a more frequent basis.

Agencies are strongly encouraged to provide additional context to their response (for example, populations or assets or users that have been excluded and the reasons why) or information about a mitigating control, where applicable. OMB and CISA are willing to work directly with agency partners with clarifying questions with the ultimate goal of enhancing security, not just obtaining compliance.

OMB defines the expected level of performance for these metrics as “adequate security,” where an agency secures its enterprise at a level commensurate with the risks associated for each system. All Federal agencies, including small agencies, should report on the status of all metrics as often as necessary to ensure that agency leadership has useful, up to-date information on the level of performance and existing gaps in their cybersecurity posture.

1 IDENTIFY

The goal of the Identify metrics section is to assist agencies with their inventory of the hardware and software systems and assets that connect to their networks. Identifying these systems and assets helps agencies facilitate their management of cybersecurity risks to systems, assets, data, and capabilities. Additionally, implementing Continuous Diagnostics and Mitigation (CDM) solutions should allow agencies to automatically detect and inventory many of these systems and assets.

- 1.1. For each [FIPS 199](#) impact level, what is the number of operational [unclassified information systems](#) by organization (i.e. Bureau or Sub-Department Operating Element) categorized at that level? (Organizations with fewer than 5,000 users may report as one unit.) ([NIST SP 800-60](#), [NIST 800-53r4 RA-2](#))

| FIPS 199 Category | 1.1.1. Organization- Operated Systems | | | 1.1.2. <u>Contractor- Operated Systems</u> | | | 1.1.3. Systems (from 1.1.1. and 1.1.2.) with Security ATO | | | 1.1.4. Systems (from 1.1.3.) that are in Ongoing Authorization ¹ | | |
|---------------------------------------|--|---|---|---|---|---|---|---|---|---|---|---|
| | H | M | L | H | M | L | H | M | L | H | M | L |
| Reporting Organization 1 | | | | | | | | | | | | |
| Reporting Organization 2 | | | | | | | | | | | | |
| [Add rows as needed for organization] | | | | | | | | | | | | |

1.1.5. Number of High Value Asset (HVA) systems reported to the BOD 18-02 data call in CyberScope this quarter². (Provided by HVA PMO)

1.1.6. Number of HVA systems (from 1.1.5.) that reside on the [organization’s unclassified network\(s\)](#).

¹ Ongoing authorization and continuous monitoring as defined in [NIST SP 800-37 Rev 2](#).

² [Binding Operational Directive BOD 18-02 Securing High Value Assets](#)

- 1.2. Number of [hardware assets](#) connected to the organization’s [unclassified network\(s\)](#).
 (Note: 1.2. is the sum of 1.2.1. through 1.2.3.) ([NIST 800-53r4 CM-8](#))

| Asset Type | Number of assets connected to the organization’s unclassified network(s). |
|---|---|
| 1.2.1. GFE endpoints | |
| 1.2.2. GFE networking devices | |
| 1.2.3. GFE input/output devices | |
| 1.2.4. GFE hardware assets (from 1.2.1 – 1.2.3.) covered by an automatic hardware asset inventory capability (e.g. scans/device discovery processes) at the enterprise-level | |
| 1.2.5. GFE endpoints (from 1.2.1.) covered by an automated software asset inventory capability at the enterprise-level | |
| 1.2.6. Number of GFE hardware assets (from 1.2.1-1.2.3) that are IPv6 enabled | |

- 1.3. Please complete the table below for mobile devices.

| | GFE | Non-GFE (e.g. Bring Your Own Device (BYOD) Assets) |
|--|---------------|---|
| Number of mobile devices . | Metric 1.3.1. | Metric 1.3.2. |
| Number of mobile devices operating under enterprise-level mobile device management that includes, at a minimum, agency defined user authentication requirements on mobile devices and the ability to remotely wipe and/or remove agency data from the devices. | Metric 1.3.3. | Metric 1.3.4. |
| Number of managed mobile devices from 1.3.3. (GFE) or 1.3.4. (BYOD) where users are unable to remove their mobile device management (MDM) or enterprise mobility management (EMM) profile without administrator approval. (NIST 800-53r4 CM-5) | Metric 1.3.5. | Metric 1.3.6. |
| Number of managed mobile devices from 1.3.3. (GFE) or 1.3.4. (BYOD) where the agency enforces the capability to deny access to agency enterprise services (through the MDM or EMM policy) when security and operating system updates have not been applied within a given period of time based on agency policy or guidance. | Metric 1.3.7. | Metric 1.3.8. |
| Number of managed mobile devices from 1.3.3. (GFE) or 1.3.4. (BYOD) where the agency enforces the capability to prevent | Metric 1.3.9. | Metric 1.3.10. |

| | | |
|--|----------------|----------------|
| the execution of unauthorized software (e.g., deny list, approve list, or cryptographic containerization) through the MDM or EMM. (NIST 800-53r4 CM-7) | | |
| Number of managed mobile devices from 1.3.3. (GFE) or 1.3.4. (BYOD) that require derived PIV credentials for mobile device transactions (e.g., authentication, secure email). (NIST SP 800-63-3) (OMB M-19-17) | Metric 1.3.11. | Metric 1.3.12. |
| What percent of your mobile devices (GFE and BYOD) are covered by a mobile threat defense (MTD) solution? (NIST SP 800-124 Rev.2) | Metric 1.3.13. | Metric 1.3.14. |

1.4. Report the types of Cloud Services³ your agency is using by cloud service provider(s) and service(s) you are receiving. (e.g., mail, database, etc.). ([NIST SP 800-145](#))

| Cloud Service Provider | Cloud Service Offering | Agency ATO Date | Sub-Agency | Service | Service Type (Drop Down) |
|------------------------------|------------------------|-----------------|--------------|-----------------------------------|--------------------------|
| Ex. Microsoft | Office 365 | 8/21/19 | Headquarters | Email and collaboration solutions | IaaS |
| <i>Add rows as necessary</i> | | | | | |

³ Cloud Services as defined by [NIST SP 800-145](#).

2 PROTECT

The goal of the Protect metrics section is to ensure that agencies safeguard their systems, networks, and facilities with appropriate cybersecurity defenses. The protect function supports agencies' ability to limit or contain the impact of potential cybersecurity events.

- 2.1. Number of devices on the network (from [1.2.](#)) assessed for vulnerabilities by a solution centrally visible at the [enterprise-level](#) that is Security Content Automation Protocol (SCAP) validated or uses National Vulnerability Database (NVD) information. ([NIST 800-53r4 RA-5](#), [NIST SP 800-128](#))
- 2.2. Please complete the table. Future configurations will be added as needed. ([NIST 80053r4 CM-8](#))

| List of top U.S. Government Operating Systems. | 2.2.1. Number of GFE hardware assets with each OS. | 2.2.2. Number of assets in 2.2.1. covered by auditing for compliance with common security configuration baselines. |
|--|--|--|
| Windows 10.x | | |
| Windows 8.x | | |
| Windows 7.x <i>Unsupported</i> | | |
| Windows Vista <i>Unsupported</i> | | |
| Windows XP <i>Unsupported</i> | | |
| Windows Server 2019 | | |
| Windows Server 2016 | | |
| Windows Server 2012 | | |
| Windows Server 2008 <i>Unsupported</i> | | |
| Windows Server 2003 <i>Unsupported</i> | | |
| Linux (all versions) | | |
| Unix/Solaris (all versions) | | |
| Mac OS X (all versions) | | |
| Other | | |
| <u>Mobile Devices</u> | | |
| Windows Mobile (all versions) | | |
| Apple iOS (all versions) | | |
| Android OS (all versions) | | |
| Blackberry OS (all versions) | | |
| Other | | |

Unprivileged and Privileged Network Users

- 2.3. Percent (%) of Privileged users with organization network accounts that have a technical control limiting access to only trusted sites.⁴
- 2.4. Please complete the table below for Unprivileged Users. ([NIST 800-53r4 IA-2\(2\)](#), [NIST SP 800-63](#))
- 2.5. Please complete the table below for Privileged Users. ([NIST 800-53r4 IA-2\(1\)](#), [NIST SP 800-63](#))

| | Unprivileged Users | Privileged Users |
|--|--------------------|------------------|
| Number of users with organization network accounts. ⁵ (Exclude non-user accounts) | Metric 2.4.1. | Metric 2.5.1. |
| Number of users (from 2.4.1. and 2.5.1.) that are required to authenticate to the network through using a two-factor PIV credential ⁶ or other Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential. ⁷ | Metric 2.4.2. | Metric 2.5.2. |
| Number of users (from 2.4.1. and 2.5.1.) that use a username and password as their primary method for network authentication ⁸ . Please describe compensating controls for limiting these users' access in the comments field. | Metric 2.4.3. | Metric 2.5.3. |
| Number of users (from 2.4.1. and 2.5.1.) covered by a centralized dynamic access management solution that controls and monitors users' access ⁹ . | Metric 2.4.4. | Metric 2.5.4. |
| Number of users (from 2.4.2. and 2.5.2.) that authenticate to the network through user-based enforcement (UBE). | Metric 2.4.5. | Metric 2.5.5. |

⁴ A trusted site is a website that has been approved by agency security officials.

⁵ An unprivileged network account is any account that is not a [privileged network account](#).

⁶ For a person with one or more unprivileged network accounts, the person should be counted in the total only if a two-factor PIV Credential is necessary to authenticate to all network accounts. The enforcement of authentication may be accomplished via either user-based or machine-based configuration settings.

⁷ For additional information, refer to [NIST SP 800-63](#).

⁸ Do not include the temporary use of username/passwords (e.g., lost or forgotten PIV cards, etc.)

⁹ Guidance on collecting metrics 2.4.4. and 2.5.4. can be found [here](#).

Network and Local System Accounts

2.6. Report the number of users with [privileged local system accounts](#) in the table below. ([NIST 800-53r4 IA-2\(3\)](#))

| | All Users |
|---|-----------------------------|
| Number of users with privileged local system accounts . | Metric 2.6.1. ¹⁰ |
| Number of users with privileged local system accounts (from 2.6.1.) that can access the Agency’s network and are required to authenticate to the network through machine-based or user-based enforcement of a two-factor PIV credential or other IAL3/AAL3 credential. | Metric 2.6.2. |

2.7. Report the number of HVA systems¹¹ (from 1.1.5.) that require all organizational users (100% privileged and unprivileged) to authenticate through the [machine-based or user based enforcement](#) of a two-factor PIV credential or other IAL3/AAL3 credential. ([DHS BOD 18-02](#) , [NIST SP 800-63](#))

2.7.1. Number of HVA systems assessed by CISA, a third-party, or independent entity (per OMB M-19-03) that determined machine-based or user-based enforcement of a two-factor PIV credential (as described in [2.7.](#)) is not required due to system architecture or mitigating security capabilities or the system’s technology is incapable of supporting this capability (e.g., industrial control systems).

Data Protection

2.8. Number of HVA systems (from 1.1.5.) that encrypt all Federal Information at rest ([OMB Circular A-130](#) Appendix I, [NIST SP 800-53r4 SC-28](#)).

2.8.1. Number of HVA systems assessed by CISA, a third-party, or independent entity (per OMB M-19-03) that determined encrypting data at rest is not required due to mitigating security capabilities or the system’s technology is incapable of supporting this capability (e.g., industrial control systems).

2.9. Number of HVA systems’ (from 1.1.6.) network is segmented from other accessible systems and applications in the agency’s network(s).

2.9.1. Number of HVA systems (from 1.1.6.) assessed by CISA, a third-party, or independent entity (per OMB M-19-03) that determined segmentation is not required due to mitigating security capabilities.

¹⁰ Do not report [privileged local system accounts](#) that are not accessible on the network.

¹¹ HVA as defined in OMB and DHS guidance. OMB will leverage existing data sources for the denominator of HVA related metrics.

Remote Access and Removable Media

- 2.10. For the [remote access connection](#) methods identified below, report the percentage utilizing FIPS 140-2 validated cryptographic modules. ([NIST 800-53r4 AC-17, SC-28\(1\)](#))
- 2.10.1a VPN
- 2.10.1b VDI/RDP
- 2.11. Number of [GFE endpoints](#) and [mobile devices](#) (from [1.2.1.](#) and [1.3.1.](#)) allowed by the agency to connect to the organization’s unclassified network via remote access (as described in 2.10).
- 2.12. Number of [GFE endpoints](#) (from [1.2.1.](#)) covered by automated mechanism to prevent the usage of untrusted removable media. ([NIST SP 800-53r4 MP-2](#))
- 2.13. Number of HVA systems (from 1.1.5) covered by an automated mechanism to determine the state of information system components with regard to flaw remediation (i.e., software patching). ([NIST SP 800-53r4 SI-2\(1\), SI-2\(2\)](#))
- 2.13.1. Number of HVA systems (from 1.1.6.) that feed flaw remediation state data into a central, [enterprise-level](#) solution. ([NIST SP 800-53r4 SI-2\(1\), SI-2\(2\), OMB M-19-03](#))
- 2.14. Number of HVA systems with adversarial testing performed within the last year (365 days). ([NIST SP 800-53r4 CA-8, CA-8\(2\)](#))

Security Training and Testing

- 2.15. Complete the table below to detail the number of users that participated in training exercises to increase awareness and/or measure effectiveness of awareness of phishing in the previous quarter (e.g. agency sends spoofed phishing emails to users and clicking links leading to phishing information page). ([OMB M-07-16](#), [NIST SP 800-53r4 AT-2](#), [NIST SP 800-16r1](#))

| Number of Users Involved | Targeted Community | Brief Summary of Test Procedures | Number of Users Who Successfully Passed ¹² the Exercise | Number of Users that Reported to Appropriate Authority | Test Date |
|------------------------------|----------------------|---|--|--|------------|
| Ex. 45 | System Administrator | Test Sys Admins’ awareness of active phishing campaigns | 15 | 9 | 11/14/2020 |
| <i>Add rows as necessary</i> | | | | | |

¹² Pass/fail criteria should be established by the agency based on the nature and intent of the test.

3 DETECT

The goal of the Detect metrics is to assess the extent that the agencies are able to discover cybersecurity events in a timely manner. Agencies should maintain and test intrusion-detection processes and procedures to ensure they have timely and adequate awareness of anomalous events on their systems and networks.

Intrusion Detection and Prevention

- 3.1. Percentage (%) of second-level agency-owned domains and mail sending hosts with DMARC set to “reject.” ([DHS BOD 18-01](#)) (Provided by CISA)
- 3.2. Percent (%) of incoming email traffic analyzed for suspicious or potentially malicious attachments without signatures that can be tested in a sandboxed environment or detonation chamber.¹³ ([NIST SP 800-53r4 SI-3](#))
- 3.3. Number of [GFE endpoints](#) (from [1.2.1.](#)) covered by an intrusion prevention system, where actions taken by the system are centrally visible at the [enterprise-level](#).¹⁴ ([NIST SP 800-53r4 SI-4](#))
- 3.4. Number of [GFE endpoints](#) (from [1.2.1.](#)) covered by an antivirus (AV) solution that provides file reputation services that check suspicious files against continuously updated malware information in near real-time. ([NIST SP 800-53r4 SI-3\(2\)](#), [NSA Slick Sheet: Anti-Virus File Reputation Services](#))
- 3.5. Number of [GFE endpoints](#) (from [1.2.1.](#)) covered by a capability that protects memory from unauthorized code execution (e.g., Data Exploitation Prevention (DEP), Address Space Layout Randomization (ASLR)). ([NIST SP 800-53r4 SI-16](#))
- 3.6. Number of [GFE endpoints](#) (from [1.2.1.](#)) protected by a browser-based or enterprise-based tool to block known phishing websites and IP addresses. ([NIST SP 800-45](#))
- 3.7. Number of assets (from [2.11.](#)) scanned for malware prior to an allowed [remote access connection](#) to the [unclassified network](#).¹⁵ ([NIST SP 800-53r4 SI-4](#))

Exfiltration and Enhanced Defenses

- 3.8. Percent (%) of outbound communications traffic checked at the external boundaries to detect potential unauthorized exfiltration of information (e.g. anomalous volumes of data, anomalous traffic patterns, elements of PII, etc.) with a solution that is centrally visible at the [enterprise-level](#). ([NIST SP 800-53r4 SI-4\(4\)](#), [SI4\(18\)](#), [SC-7\(10\)](#))

¹³ It is not necessary to be able to simultaneously inspect all email traffic within a segregated environment in order to respond with 100%. To respond 100%, all emails must be analyzed, and the agency must have the capability to segregate suspicious email for investigation as needed.

¹⁴ Intrusion prevention systems include both host and network-based instances for the purpose of this question.

¹⁵ In addition to scanning at the time of device connection, for the purposes of this metric, it is additionally appropriate if the device last scan date is checked and complies with organization policies.

Network Defense

- 3.9. Percent (%) of the organization's unclassified network¹⁶ that has implemented a technology solution centrally visible at the [enterprise-level](#) to detect and alert on the connection of unauthorized hardware assets. ([NIST SP 800-53r4 SI-4 \(4\)\(18\)](#), [SC-7\(10\)](#))
 - 3.9.1. Mean time to detect a new device (time between scans in [3.9.](#)).
 - 3.9.2. Percent (%) of the organization's unclassified network that has implemented a technology solution centrally visible at the enterprise-level to block network access of unauthorized hardware assets.
- 3.10. Number of GFE endpoints (from [1.2.1.](#)) covered by a software asset management capability centrally visible at the [enterprise-level](#) that is able to detect unauthorized software and alert appropriate security personnel. ([NIST SP 800-53r4 CA-7](#), [CM-7\(5\)](#), [RA-5](#), [NIST SP 800-128](#))
 - 3.10.1. Number of GFE endpoints (from [1.2.1.](#)) covered by a software asset management capability centrally visible at the enterprise-level that is enabled to block or prevent unauthorized software from executing (e.g., certificate, path, hash value, services, and behavior based allow listing solutions).

¹⁶ For the purposes of accurately identifying a weighted percentage, agencies may use a base of the value reported for 1.2.; use a base of total organization assigned IP addresses; or use other agency-defined method that is consistently reported and accurately reflects the weighting of agency networks.

4 RESPOND

The goal of the Respond metrics is to ensure that agencies have policies and procedures in place that detail how their enterprise will respond to cybersecurity events. Agencies should develop and test response plans and communicate response activities to stakeholders to minimize the impact of cybersecurity events, when they occur.

- 4.1. Mean time for the organization to detect system intrusion or compromise over the prior 12 months (past 365 days). Please include time and units (seconds, minutes, hours, days). If not applicable, please note one of the following: “Not applicable; no intrusions or compromises”, “Not applicable; capability to measure does not exist”, “Not applicable; capability exists but is not sufficiently mature.”
 - 4.1.1. Mean time for the organization to contain a system intrusion or compromise after detection over the prior 12 months (past 365 days). Please include time and units (seconds, minutes, hours, days). If not applicable, please note one of the following: “Not applicable; no intrusions or compromises”, “Not applicable; capability to measure does not exist”, “Not applicable; capability exists but is not sufficiently mature.”
- 4.2. Percent (%) of the organization’s unclassified network¹⁷ covered by an automated mechanism to assist in the tracking of security incidents and the collection and analysis of incident information. ([NIST SP 800-53r4 IR-5\(1\)](#), [NIST SP 800-61](#))
- 4.3. Number of HVA systems covered by a capability that can dynamically reconfigure and/or automatically disable the system or relevant asset upon the detection of a given security violation or vulnerability.¹⁸ [NIST SP 800-53r4, IR-4\(2\), IR-4\(5\)](#).

¹⁷ For the purposes of accurately identifying a weighted percentage, agencies may use a base of the value reported for 1.2.; use a base of total organization assigned IP addresses; or use other agency-defined method that is consistently reported and accurately reflects the weighting of agency networks.

¹⁸ Potential security violations and vulnerabilities for HVA systems is left to agency discretion.

5 RECOVER

The goal of the Recover metrics is to ensure agencies develop and implement appropriate activities for resilience that allow for the restoration of any capabilities and/or services that were impaired due to a cybersecurity event. The recover function reduces the impact of a cybersecurity event through the timely resumption of normal operations.

- 5.1. Number of HVA systems 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 800-53r4 CP-2\(1\)](#), [NIST SP 800-34](#))
 - 5.1.1. Number of HVA systems (from 5.1.) that have an alternate processing site identified and provisioned, operate multiple redundant sites for resiliency, or that can be provisioned within the organization-defined time period for resumption. ([NIST SP 800-53r4 CP-7\(4\)](#))
- 5.2. Mean time for the organization to restore operations following the containment of a system intrusion or compromise over the prior 12 months (past 365 days). Please include time and units (seconds, minutes, hours, days). If not applicable, please note one the following: “Not applicable; no intrusions or compromises”, “Not applicable; capability to measure does not exist”, “Not applicable; capability exists but is not sufficiently mature.”

APPENDIX A: SUMMARY OF FISMA CAP GOAL TARGETS & METHODOLOGY

Appendix A provides a summary of the FISMA CAP Goal Metric Targets and methodology for Information Security Continuous Monitoring (ISCM), Strong Authentication (ICAM), and Advanced Network and Data Protections (ANDP).

| Summary of FISMA CAP Goal Targets & Methodology | | | |
|---|----------|--|--|
| Capability | Target % | FY 2021 Annual FISMA CIO Metrics | Agency Calculation |
| Information Security Continuous Monitoring (ISCM) | | | |
| Software Asset Management | ≥ 95% | 1.2.1, 3.10. | 95% Implementation |
| Hardware Asset Management | ≥ 95% | 3.9. | 95% Implementation |
| Authorization Management | 100% | 1.1. | 100% of High Impact Systems Authorized and 100% of Moderate Impact Systems Authorized |
| Mobile Device Management | 95% | 1.3., 1.3.1., 1.3.2., 1.3.3., 1.3.4. | 95% Implementation |
| Identity, Credential, and Access Management (ICAM) | | | |
| Privileged Network Access Management | 100% | 2.5.1., 2.5.2. | 100% Implementation |
| HVA System Access Management | ≥ 90% | 1.1., 2.7. | 90% Implementation |
| Automated Access Management | ≥ 95% | 2.4.1., 2.4.4., 2.5.1., 2.5.4. | 95% Implementation |
| Advanced Network and Data Protections (ANDP) | | | |
| Intrusion Detection and Prevention | ≥ 90% | 3.1.,3.2., 3.3., 3.4., 3.5., 3.6., 3.7. | DMARC is 100%, and at least 4 of 6 other metrics have met an implementation target of at least 90% |
| Exfiltration and Enhanced Defenses | ≥ 90% | 3.8. | 90% implementation |
| Data Protection | ≥ 90% | 2.8., 2.9., 2.10.1., 2.12., 2.13., 2.13.1. | At least 4 of 6 metrics have met an implementation target of at least 90% |

APPENDIX B: DEFINITIONS

Adversarial Testing

Organizations can use adversarial testing to inform themselves of the exploitable vulnerabilities inherent to their network. This testing can be described as Red Team, Penetration Testing, Application testing, or in other terms. In the same way that Continuous Diagnostics and Mitigation can discover previously unknown vulnerabilities, periodic adversarial testing can help organizations identify and mitigate potential risk before it is exploited with malicious intent. For this reason, it is important for all organizations to consider this as part of their risk management program.

Centrally visible at the enterprise-level

Information collected or consolidated by tools or solutions is transmitted via an automated process to a single centralized, continuously reviewed dashboard, report, or alert mechanism with purview over the entire enterprise.

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.¹⁹

Controlled Unclassified Information (CUI)

information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government -wide policies, excluding information classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

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)

Enterprise-level

The entire reporting organization that includes each organizational component with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance.

Government Furnished Equipment (GFE)

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

¹⁹ See 44 USC 3554(a)(1)(A)), [NIST SP 800-171](#)

- Endpoints:²⁰
 - Servers (including mainframe/minicomputers/midrange computers)
 - Workstations (desktops laptops, Tablet PCs, and net-books)
 - Virtual machines that can be addressed²¹ as if they are a separate physical machine should be counted as separate assets,²² including dynamic and on demand virtual environments
- Mobile devices:
 - Smartphone
 - Tablets
 - Pagers
- Networking devices:²³
 - 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 infrastructure²⁴
 - 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

²⁰ A multi-purpose device needs to be counted only once. A device with multiple IP connections needs to be counted only once, not once per connection. This is an inventory of hardware assets, not data.

²¹ “Addressable” means by IP address or any other method to communicate to the network.

²² 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. (Things like multiple CPUs, on the other hand, do not create separate assets, generally, because the CPUs are not addressable and are subject to attack only as part of the larger asset). If you have issues about how to apply this for specific cloud providers, please contact FedRAMP for further guidance: <http://fedramp.gov>.

²³ This list is not meant to be exhaustive, as there are many types of networking devices. If the devices are connected, they are to be included.

²⁴ PKI assets should be counted as constituent assets on networks in which they reside.

Both GFE assets and non-GFE assets are included if they meet the other criteria for inclusion listed here.²⁵ 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.

Incident

A violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard security practices (NIST SP 800-61 Rev2).

Information system(s)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Contingency Plan (ISCP)

An ISCP provides established procedures for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system.

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.

Local system account

A predefined local account used by service control manager that has extensive privileges on a local system.²⁶

Mean time

The sum of time between detections divided by the number of detections.

Mobile device

A portable computer device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g. by wirelessly transmitting or receiving information); (iii) possess local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.

²⁵ 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.

²⁶ [https://msdn.microsoft.com/en-us/library/windows/desktop/ms684190\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms684190(v=vs.85).aspx)

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.²⁷

Network Access

Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Network Account

A user account that provides access to the network.

Non-user account

An account that is not intended to be controlled directly by a person (or group). The account is either (a) intended to be used by the system or an application, which presents credentials and performs functions under the management of the person (or group) that owns the account, or (b) created to establish a service (like a group mailbox), and no one is expected to log into the account.

Organization Network

The interconnected information systems or components controlled by an organization or trusted to communicate without having traffic inspected by a trusted intermediary (e.g., Trusted Internet Connection (TIC) or Managed Trusted Internet Protocol Services (MTIPS) provider).

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). The Federal standard for this is specified as Federal Information Processing Standard Publication 201 (FIPS 201).

Privileged local system account

A user account with elevated privileges which is typically allocated to system administrators, database administrators, developers, and others who are responsible for system/application control, monitoring, or administration functions. In Linux or other Unix-like operating systems, these are typically referred to as root account, root user, or super-user accounts.

Privileged network account

A network account with elevated privileges, which is typically allocated to system administrators, network administrators, and others who are responsible for system/application control, monitoring, or administration functions.

²⁷ <https://csrc.nist.gov/Glossary/?term=233#AlphaIndexDiv>

Public key infrastructure (PKI)

A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Remote access

The ability for an organization's users to access its non-public computing resources from locations external to the organization's facilities.

Remote access connections

An external connection that allows access to the organization's internal/private network utilizing one of the remote access connection methods described in Metric 2.10.

Remote desktop protocol (RDP)

A protocol (developed by Microsoft) that allows a user the ability to use a graphical interface over a network connection.

Segmented

Physically, logically, or virtually separated from the general computational environment by controlled access through a managed interface.

Sender authentication protocols

Protocols to validate the identity of email senders and protect against forgery of those identities, including:

- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)
- Sender Policy Framework (SPF)

Smart phone

A mobile phone built on a mobile computing platform, with more advanced computing ability and connectivity than a contemporary feature phone.

Successful phishing attack

A network user responds to a fraudulent message producing a negative impact on confidentiality, integrity, and/or availability of the organization's information.

Unclassified information system(s)

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

Unclassified network

A collection of interconnected components 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.

Unprivileged Network Account

An unprivileged network account is any account that is not a privileged network account, also known as a standard account.

Virtual desktop infrastructure (VDI)

A server or collection of servers that allow the ability to host multiple guest desktop operating systems for end-users.

Virtual machine

Software that allows a single host to run one or more guest operating systems.

Virtual private network (VPN)

A connection that allows the Agency to extend their internal/private network to a remote location through an untrusted network (e.g., Internet).