# FY 2018 CIO FISMA Metrics

Version 1.0
31 October 2017

*This page is intentionally left blank*

# Table of Contents

# GENERAL INSTRUCTIONS

## Responsibilities

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.

## Overview and Purpose

The Fiscal Year (FY) 2018 Chief Information Officer (CIO) FISMA 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.

Since FY 2016, OMB and the Department of Homeland Security (DHS) 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 Guide for Applying the Risk Management Framework to Federal Information Systems, 800-39, Managing Information Security Risk: Organization, Mission, and Information System View* and associated standards and guidelines, provides agencies with a comprehensive structure for making more informed, risk-based decisions and managing cybersecurity risks across their enterprise.

## Expected Levels of Performance

Agencies should view the target levels for the FY 2018 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 OMB M-18-02. 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 targets (Appendix A). These reporting requirements also fulfill the requirement for agencies to

conduct regular risk management assessments established in Executive Order (EO) 13800 "*Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*." OMB will also provide guidance to agencies in the event that OMB requires agencies to report on their performance on a more frequent basis.

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 (OMB M-11-33, FAQ 15). 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)

| | 1.1.1. Organization-Operated Systems | | | 1.1.2. Contractor-Operated Systems | | | 1.1.3. Government Shared Service Provider-Operated Systems[1] | | | 1.1.4. Systems (from 1.1.1. and 1.1.2.) with Security ATO[2] | | | 1.1.5. Systems (from 1.1.4.) that are in Ongoing Authorization[3] | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **FIPS 199 Category** | **H** | **M** | **L** | **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] Please identify shared services that your organization is providing to external agencies. For shared services leveraged by your agency, please report them in Metric 1.5.
[2] For this metric, agencies should consider government shared services for which customer agencies have issued an Authority to Use as having a security ATO.
[3] Ongoing authorization and continuous monitoring as defined in NIST SP 800-37 Rev 1.

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 1.2.4.) (OMB M-18-02, 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 mobile devices | |
| 1.2.3. GFE networking devices | |
| 1.2.4. GFE input/output devices | |
| 1.2.5. GFE hardware assets (from 1.2.1 – 1.2.4.) covered by an automatic hardware asset inventory capability (e.g. scans/device discovery processes) at the enterprise-level | |
| 1.2.6. GFE endpoints and mobile devices (from 1.2.1. and 1.2.2.) covered by an automated software asset inventory capability at the enterprise-level | |
| 1.2.7. Non-GFE endpoints | |

1.3. Date of the most recent update to the enterprise-level mobile device management policy. (NIST SP 800-124r1, NIST SP 800-46r2, NIST 800-53r4 AC-19)

1.3.1. Number of Non-GFE mobile devices. (e.g. Bring Your Own Device (BYOD) Assets)

1.3.2. Number of mobile assets (from 1.2.2. and 1.3.1) operating under an enterprise-level mobile device management policy that includes, at a minimum, agency defined user authentication requirements on mobile devices and the ability to remotely wipe mobile devices.

1.3.3. Does the organization possess one or more separate, external, dedicated networks for non-GFE BYOD use within enterprise facilities? (e.g., guest wireless network)

1.4. Report the types of Cloud Services[4] 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 | 2/21/15 | Headquarters | Email and collaboration solutions | IaaS |
| *Add rows as necessary* | | | | | |

[4] Cloud Services as defined by NIST SP 800-145

1.5. Report the types of Federal government-provided shared services your agency is using by service provider(s) and service(s) you are receiving. (e.g., mail, database, etc.) OMB M-16-11)

| Shared Service Provider | Shared Service Offering | MOU Date | Sub-Agency | Service | Service Type (Drop Down) |
|---|---|---|---|---|---|
| Ex. USDA | WebTA | 2/21/15 | Headquarters | Employee Time and Attendance | IaaS |
| *Add rows as necessary* | | | | | |

1.6. Date of issuance of or most recent update to enterprise-level Risk Management Plan that includes cybersecurity/information security risks. (OMB Circular A-123)

1.6.1. Date of issuance of enterprise-level policy, if different than enterprise risk management plan, empowering incident commanders to direct and manage cybersecurity incidents.

# 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 using Security Content Automation Protocol (SCAP) validated products or solutions with 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 800-53r4 CM-8)

| List of top U.S. Government Operating Systems. | 2.2.1. Number of GFE hardware assets with each OS. | 2.2.2. The common security configuration baseline for each OS listed. (e.g., USGCB) | 2.2.3. Number of assets in 2.2.1. covered by auditing for compliance with 2.2.2. |
|---|---|---|---|
| Windows 10.x | | | |
| Windows 8.x | | | |
| Windows 7.x | | | |
| Windows Vista *Unsupported* | | | |
| Windows XP *Unsupported* | | | |
| Windows Server 2016 | | | |
| Windows Server 2012 | | | |
| Windows Server 2008 | | | |
| Windows Server 2003 *Unsupported* | | | |
| Linux (all versions) | | | |
| Unix/Solaris (all versions) | | | |
| Mac OS X (all versions) | | | |
| **Mobile Devices** | | | |
| Windows Mobile (all versions) | | | |
| Apple iOS (all versions) | | | |
| Android OS (all versions) | | | |
| Blackberry OS (all versions) | | | |

## Identity and Access Management

2.3. Date of issuance of an enterprise-level Identity, Credential, and Access Management policy. (OMB Circular A-130, Homeland Security Presidential Directive 12 (HSPD-12), NIST SP 800-53r4 AC-6(7))

2.3.1. Enterprise-level Identity, Credential, and Access Management policy contains processes for the review of user privileges, provisioning privileges upon entry, revoking privileges upon exit, and modifying privileges based on changes in duties. (e.g. role based access control).

## Unprivileged and Privileged Network Users

2.4. Please complete the table below for Unprivileged Users. (OMB M-18-02, NIST 800-53r4 IA-2(2), NIST SP 800-63)

2.5. Please complete the table below for Privileged Users. (OMB M-18-02, NIST 800-53r4 IA-2(1), NIST SP 800-63)

| | Unprivileged Users | Privileged Users |
|---|---|---|
| Number of users with 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 the machine-based or user-based enforcement of a two-factor PIV credential[6] or other NIST 800-63 r3 Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3/Federated Assurance Level (FAL) 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. 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. (NIST SP 800-53r4 AC-2(6)) | Metric 2.4.4. | Metric 2.5.4. |
| Frequency with which user privileges are reviewed, according to agency policy. | | Metric 2.5.5. |
| Percent (%) of users with network accounts that have a technical control limiting access to only trusted sites.[8] | | Metric 2.5.6. |

[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] A trusted site is a website that has been approved (i.e., whitelisted) by agency security officials.

## 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.[9] |
| Number of users with privileged local system accounts (from 2.6.1) are accessible through the Agency's network in which the privileged user is required to authenticate to the network through the machine-based or user-based enforcement of a two-factor PIV credential or other NIST 800-63 r3 IAL3/AAL3/FAL3 credential. | Metric 2.6.2. |

2.7. Report the number of network accounts assigned to unprivileged and privileged users in the table below. (NIST 800-53r4 IA-2(1), IA-2(2))

2.8. Report the number of local system accounts assigned to unprivileged and privileged users in the table below. (NIST 800-53r4 IA-2(1), IA-2(2))

| | Unprivileged Users | Privileged Users |
|---|---|---|
| Number of network accounts assigned to users. (Exclude non-user accounts.) | Metric 2.7.1. | Metric 2.7.2. |
| Number of local system accounts assigned to users. | Metric 2.8.1. | Metric 2.8.2. |

## Data Protection

2.9. Report the number of systems with the following properties. (OMB M-18-02, NIST SP 800-63)

| | High Impact Systems | Moderate Impact Systems | Low Impact Systems |
|---|---|---|---|
| Number of systems (from 1.1.) that require all users (100% privileged and 100% unprivileged) to authenticate through the machine-based or user-based enforcement of a two-factor PIV credential or other NIST 800-63 r3 IAL3/AAL3/FAL3 credential. | Metric 2.9.1. | Metric 2.9.2. | Metric 2.9.3. |
| Number of systems (from 1.1.) that encrypt data at rest. | Metric 2.9.4. | Metric 2.9.5. | Metric 2.9.6. |
| Number of systems (from 1.1.) that are segmented from other accessible systems and applications in the | Metric 2.9.7. | | |

[9] Do not report privileged local system accounts that are not accessible on the network.

| | High Impact Systems | Moderate Impact Systems | Low Impact Systems |
|---|---|---|---|
| agency's network(s). | | | |

## Remote Access and Removable Media

2.10. For the remote access connection methods identified below, report the percentage that have each of the following properties. (NIST 800-53r4 AC-17, SC-7(7)SC-10, SC-28(1), SC-10))

| Connection Method Type | VPN | VDI/ RDP | Dial up or other (without VPN) |
|---|---|---|---|
| 2.10.1. Percent (%) utilizing FIPS 140-2 validated cryptographic modules. | % or NA | % or NA | |
| 2.10.2. Percent (%) configured in accordance with OMB M-07-16 to time out after 30 minutes (or less) of inactivity and requires re-authentication to re-establish a session. | % or NA | % or NA | |
| 2.10.3. Percent (%) prohibiting the use of split tunneling and/or dual-connected remote hosts where the connecting device has two active connections. | % or NA | | % or NA |
| 2.10.4. Number of GFE endpoints and mobile devices (from 1.2.1. and 1.2.2.) authorized for remote access connection to the unclassified network. | | | |

2.11. Date of issue or last update to enterprise-level policy defining and prohibiting the use of untrusted removable media. (NIST SP 800-53r4 MP-7)

2.11.1. Number of GFE endpoints (from 1.2.1.) covered by automated mechanism to prevent the usage of untrusted removable media.

2.12. Date of issuance of an enterprise-level policy for destroying media containing sensitive information in line with the specifications outlined in NIST SP 800-88r1.

2.13. Number of systems (from 1.1.1. and 1.1.2.) 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 systems (from 2.13.) that feed into a central, enterprise-level solution.

2.14. Number of unresolved Common Vulnerabilities and Exposures (CVEs) with a critical risk score (Common Vulnerability Scoring System (CVSS) Score of 9.0 - 10.0) on high impact information systems (as identified in 1.1.) outstanding for greater than 30 days. (OMB Circular A-130)

2.14.1. Number of unresolved CVEs with a high risk score (CVSS Score of 7.0 – 8.9) on high impact information systems (as identified in 1.1.1. and 1.1.2.) outstanding for greater than 60 days.

## Security Training and Phishing Tests

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[10] 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 | 10/14/2017 |
| *Add rows as necessary* | | | | | |

## Insider Threat Program

2.16. Is your agency required to have an Insider Threat Program per Executive Order 13587 and the *National Insider Threat Policy & Minimum Standards*?[11]

2.16.1. If yes, has your Insider Threat Program been assessed by the National Insider Threat Task Force (NITTF)?

[10] Pass/fail criteria should be established by the agency based on the nature and intent of the test.
[11] https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf

# 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. Complete the table below to detail the percentage (%) of incoming and outgoing email traffic analyzed using email authentication protocols. (NIST SP 800-53r4)

| Email Authentication Protocol | % of incoming email traffic analyzed | % of outgoing email traffic analyzed |
|---|---|---|
| DKIM | | |
| DMARC | | |
| SPF | | |
| Other (please list) | | |

3.2. Percent (%) of incoming email traffic analyzed for suspicious or potentially malicious attachments against known signatures that can be tested in a sandboxed environment or detonation chamber.[12] (NIST SP 800-53r4)

3.3. Number of GFE endpoints (from 1.2.1.) covered by an intrusion prevention system.[13] (NIST SP 800-53r4)

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 anti-exploitation capabilities (e.g., Data Exploitation Prevention (DEP), Address Space Layout Randomization (ASLR)). (NIST SP 800-53r4 SI-3)

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 1.2.1. and 1.2.2.) scanned for malware prior to an authorized remote access connection to the unclassified network.[14] (NIST SP 800-53r4 SI-4)

[12] 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.
[13] Intrusion prevention systems include both host and network-based instances for the purpose of this question.
[14] 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.

## Exfiltration and Enhanced Defenses

3.8. Percent (%) of inbound network traffic that passes through a web content filter, which provides anti-phishing, anti-malware, and blocking of malicious websites. (NIST SP 800-53r4 SI-3, SI-7(8))

3.8.1. Percent (%) of outbound network traffic that passes through a web content filter that protects against distribution of malware and blocks access to known malicious websites.

3.9. Percent (%) of outbound communications traffic checked at the external boundaries to detect encrypted exfiltration of information (e.g., TLS, SSL). (NIST SP 800-53r4 SI-4 (4)(18), SC-7(10))

3.10. 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.) (NIST SP 800-53r4 SI-4(4), SI-4(18), SC-7(10))

3.11. Percent (%) of email messages processed by systems that quarantine or otherwise block suspected malicious traffic. (NIST SP 800-53r4 SC-18, SI-3)

3.12. Date of issue or last update to policy establishing procedures for testing exfiltration detection capabilities. (NIST SP 800-53r4 SC-7)

3.12.1. Date of last test exfiltration exercise and results of the exercise. (e.g., test exfiltrations were detected or not)

## Network Defense

3.13. Percent (%) of the organization's unclassified network[15] that has implemented a technology solution to detect and alert on the connection of unauthorized hardware assets. (NIST SP 800-53r4 SI-4 (4)(18), SC-7(10))

3.13.1. Mean time to detect a new device (time between scans in 3.13.).

3.14. Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) covered by a software asset management capability to detect unauthorized software, alert, and block to prevent the software from executing. (e.g., certificate, path, hash value, services, and behavior based whitelisting solutions) (NIST SP 800-53r4 CA-7, CM-7(5), RA-5), NIST SP 800-128)

[15] 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. Date of issuance of an enterprise-wide incident response plan, developed in accordance with NIST SP 800-61.

4.2. Number of computer security incidents[16] reported to agency Security Operations Centers or other appropriate agency resource this quarter (please also update the fiscal year total). (US-CERT Federal Incident Notification Guidelines)

4.2.1. Number of computer security incidents reported to US-CERT this quarter.

4.2.2. Mean time for the agency to confirm a cybersecurity incident.

4.3. Percent (%) of the organization's network 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)

4.4. Complete the table below for all High Impact systems. (NIST SP 800-53r4 IR-4(2))

4.5. Complete the table below for all Moderate Impact systems. (NIST SP 800-53r4 IR-4(5))

| | High Impact Systems | Moderate Impact Systems |
|---|---|---|
| Number of systems (from 1.1.) covered by a dynamic reconfiguration capability as part of its incident response capabilities. | Metric 4.4.1. | Metric 4.5.1. |
| Number of systems (from 1.1.) covered by a capability that can automatically disable it upon the detection of a given security violation or vulnerability. | Metric 4.4.2. | Metric 4.5.2. |

4.6 Complete the table below for all enterprise-wide incident response plans tested during the past 365 days. (NIST SP 800-61)

| Date of Test | Test Type | Brief Summary of Procedures and Results | Included Verification of Roles and Responsibilities (Y/N)? |
|---|---|---|---|
| Ex 45 | Table Top | Deputy Secretary-led incident response to breach of high impact system containing PII. | Y |

[16] FISMA (44 USC § 3552) defines a computer security incident as an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or (B) an information system; or, constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

| | | | |
|---|---|---|---|
| *Add rows as necessary* | | | |

# 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. Date of issuance or last update to a documented, approved, and disseminated enterprise-level Continuity of Operations (COOP) Plan, or similar recovery document, developed to provide procedures and guidance to sustain the Mission Essential Functions (MEFs) at an alternate site for up to 30 days. (NIST SP 800-34)

5.1.1. Date of the most recent telecommunications recovery strategy.

5.1.2. Date of the most recent update to primary and alternate telecommunications service agreements, which include priority-of-service provisions in accordance with organizational availability requirements, for the organization.

5.2. Date of issuance or last update to a Disaster Recovery Plan (per NIST Cybersecurity Framework) developed at the enterprise level and tested at least annually. (NIST SP 800-53r4)

5.3. Date of issuance or last update to an Incident Recovery Plan (per NIST Cybersecurity Framework) developed at the enterprise level and tested at least annually. (Note: the Incident Recovery Plan can be part of the Incident Response Plan, and please note whether this is the case in the comment field) (NIST SP 800-53r4)

5.4. Date of issuance or last update to enterprise-level policy detailing the minimum frequency requirement[17] for transferring backup data to an off-site facility for information systems with a high-risk availability rating per FIPS 199. (NIST SP 800-34)

5.5. Date of issuance or last update to enterprise-level Business Continuity Plan (BCP), or similar recovery document, developed to provide procedures for sustaining mission/business operations during and after a significant disruption. (NIST SP 800-34, OMB Circular A-130)

5.6. Number of high impact information systems (from 1.1) 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 800-34).

5.6.1. Number of high impact information systems (from 5.6.) that have an alternate processing site identified and provisioned.

[17] The minimum frequency requirement is the minimum regularity (i.e. daily or weekly) with which policy dictates back-up data is transferred to an off-site facility.

# 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 Anti-Phishing and Malware Defense.

| Summary of FISMA CAP Goal Targets & Methodology | | | | |
|---|---|---|---|---|
| **Capability** | **Target %** | **FY 2018 Annual FISMA CIO Metrics** | **FY 2017 Annual FISMA CIO Metrics** | **Agency Calculation** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

The Fiscal Year (FY) 2018 Cybersecurity Cross Agency Priority (CAP) Goal Targets will be identified and released by Quarter 3 of FY 2018.

The Fiscal Year (FY) 2018 Cybersecurity Cross Agency Priority (CAP) Goal Targets will be identified and released by Quarter 3 of FY 2018.

# APPENDIX B: DEFINITIONS

**Authority to Use (ATU)**
Employed when an organization (customer organization) chooses to accept information in an existing authorization package generated by another organization (provider organization).

**Business Continuity Plan (BCP)**
The BCP focuses on sustaining an organization's mission/business processes during and after a disruption. An example of a mission/business process may be an organization's payroll process or customer service process. A BCP may be written for mission/business processes within a single business unit or may address the entire organization's processes. The BCP may also be scoped to address only the functions deemed to be priorities. A BCP may be used for long-term recovery in conjunction with the COOP plan, allowing for additional functions to come online as resources or time allow. Because mission/business processes use information systems (ISs), the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and IS capabilities are matched.

**Continuity of Operations (COOP) Plan**
COOP focuses on restoring an organization's mission essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. Additional functions, or those at a field office level, may be addressed by a BCP. Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP plan. Standard elements of a COOP plan include:

- Program plans and procedures
- Continuity communications
- Risk management
- Vital records management
- Budgeting and acquisition of resources
- Human capital
- Essential functions
- Test, training, and exercise
- Order of succession
- Devolution
- Delegation of authority
- Reconstitution
- Continuity facilities

**Credentialed (Privileged) scan**
Credentialed scans grant local access to scan the target system. These authenticated network scans allow a remote network audit to obtain detailed information such as installed software, missing security patches and operating system settings. These include both external scans carrying a credential or scans by a sensor agent resident on the device, running as system or as a privileged account. A scanning agent often requires elevated privileges to read registries and access protected resources.

**Cyber Incident Response Plan (CIRP)**
A set of procedures to enable security personnel to identify, mitigate, and recover from cybersecurity attacks against an organization's information system(s).[18]

[18] For more information, please refer to NIST 800-184

**Disaster Recovery (DR) Plan**
A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.[19]

**Enterprise level**
The entire reporting organization or 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.)

- Endpoints:[20]
  - Servers (including mainframe/minicomputers/midrange computers)
  - Workstations (desktops laptops, Tablet PCs, and net-books)
  - Virtual machines that can be addressed[21] 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)

[19] For more information, please refer to NIST 800-34 Rev. 1
[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.

    - Load balancers
    - Encryptors/decryptors
    - VPN
    - Alarms and physical access control devices
    - PKI infrastructure[24]
    - 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.[25] Mobile devices that receive Federal email are considered to be connected. 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).

**Incident Recovery Plan**
The Incident Recovery Plan is part of a cyber incident response plan with a concentration on the recovery element.[26]

**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.

[24] PKI assets should be counted as constituent assets on networks in which they reside.
[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] For more information, please refer to NIST 800-184

**Local system account**
A predefined local account used by service control manager that has extensive privileges on a local system.[27]

**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.

**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. [28]

**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.

**Network Group**
A collection of users and accounts that can be managed as a single unit.

**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.

**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).

[27] https://msdn.microsoft.com/en-us/library/windows/desktop/ms684190(v=vs.85).aspx
[28] https://csrc.nist.gov/Glossary/?term=233#AlphaIndexDiv

**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.

**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**
A 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.

**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)

**Shared Account**
An account that is utilized by a group rather than an individual person. Shared accounts are not associated with a particular person.

**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 in FY 2018, 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.)