FY 2018 CIO FISMA Metrics

Version 2.0.1
May 2018
Effective FY 2018 Quarter 3

This page is intentionally left blank

Revision History

Version	Date	Comments	Authors	Sec/Page
1.0	03/2018	Initial draft of updates to FY 2018 Metrics	OMB/DHS	All
2.0	04/2018	Revisions to metrics and definitions (see General Instructions).	OMB/DHS	All
2.0.1	05/2018	Minor formatting and typo corrections.	DHS	All

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 Rev 1 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.

What's New?

Over the past few months, OMB and DHS, in collaboration with agency partners, have undertaken an effort to review the FISMA CIO metrics to ensure alignment with the priorities outlined in the *Report to the President on Federal IT Modernization*. Highlights of the changes in this update include:

- Many metrics previously counting high and moderate impact systems have been re-written to focus on HVA systems;
- Metrics concerning the existence or testing of a policy have been removed with evaluation now residing in the FY 2018 FISMA Inspectors General (IG) metrics, where IGs can assess both the existence and maturity of such policies;
- The removal of duplicative metrics or metrics not directly used to assess the degree to which agencies are managing their cybersecurity risk;
- The addition of the phrase "centrally visible at the enterprise-level" to several metrics, with the objective of ensuring that agencies have central access to the information provided by their tools without the need to make distinct manual data calls to their components; and
- The addition of metrics to measure the time to detect ('dwell time') and recover from system compromises.

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. 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]		
FIPS 199 Category	**H**	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**
Reporting Organization 1												
Reporting Organization 2												
[Add rows as needed for organization]												

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

Asset Type	Number of assets connected to the organization's unclassified network(s).
1.2.5. GFE endpoints (from 1.2.1.) covered by an automated software asset inventory capability at the enterprise-level	
1.2.6. Non-GFE endpoints	

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 assets 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.

1.4. Report the types of Cloud Services[2] 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					

[2] 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. 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)			

Unprivileged and Privileged Network Users

2.3. Percent (%) of Privileged users with network accounts that have a technical control limiting access to only trusted sites.[3]

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

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.[4] (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[5] or other Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential.[6]	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.

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.[7]

[4] An unprivileged network account is any account that is not a privileged network account.
[5] 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.
[6] For additional information, refer to NIST SP 800-63.
[7] Do not report privileged local system accounts that are not accessible on the network.

	All Users
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 the machine-based or user-based enforcement of a two-factor PIV credential or other IAL3/AAL3 credential.	Metric 2.6.2.

2.7. Number of High Value Asset (HVA) systems[8] that require all government and contractor 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. (OMB M-18-02, NIST SP 800-63)

2.7.1. Number of HVA systems where an HVA assessment (per OMB and DHS guidance) determined machine-based or user-based enforcement of a two-factor PIV credential (as described in 2.7.) is not applicable to the system architecture.

Data Protection

2.8. Number of HVA systems 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 where an HVA assessment (per OMB and DHS guidance) determined encrypting all Federal Information at rest is not applicable to the system architecture.

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

2.9.1. Number of HVA systems where an HVA assessment (per OMB and DHS guidance) determined segmentation is not applicable to the system architecture.

[8] 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 that have each of the following properties. (NIST 800-53r4 AC-17, SC-7(7), SC-10, SC-28(1))

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

2.11. Number of GFE endpoints and mobile devices (from 1.2.1. and 1.3.1) authorized for remote access connection to the unclassified network.

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

2.13. Number of HVA systems 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 2.13) that feed into a central, enterprise-level solution. (NIST SP 800-53r4 SI-2(1), SI-2(2))

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

2.14.1. Number of unique unresolved CVEs with a high risk score (CVSS Score of 7.0 – 8.9) on HVA systems 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[9] 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					

[9] 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." (Provided by DHS NCATS) (DHS BOD 18-01)

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.[10] (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.[11] (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 authorized remote access connection to the unclassified network.[12] (NIST SP 800-53r4 SI-4)

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 80053r4 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.

[10] 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.

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

[12] 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.

3.9. 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))

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

Network Defense

3.11. Percent (%) of the organization's unclassified network[13] 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))

3.11.1. Mean time to detect a new device (time between scans in 3.11.).

3.12. 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, 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)

[13] 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. Number of computer security incidents[14] 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)

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

4.1.2. 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."

4.1.3. 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 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)

4.3. Number of HVA systems covered by a capability that can automatically disable the system or relevant asset upon the detection of a given security violation or vulnerability[15] NIST SP 800-53r4 IR-4(2).

[14] 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.

[15] 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.

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 2018 Annual FISMA CIO Metrics**	**Agency Calculation**
Information Security Continuous Monitoring (ISCM)			
Software Asset Management	≥ 95%	1.2.1, 3.12	95% Implementation
Hardware Asset Management	≥ 95%	3.11	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%	3.2, 3.3, 3.4, 3.5, 3.6, 3.7	At least 4 of 6 other metrics have met an implementation target of at least 90%
Exfiltration and Enhanced Defenses	≥ 90%	3.8, 3.8.1, 3.9, 3.10	At least 3 of 4 metrics have met an implementation target of at least 90%
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

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.[16]

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.

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.)

- Endpoints:[17]
  - Servers (including mainframe/minicomputers/midrange computers)
  - Workstations (desktops laptops, Tablet PCs, and net-books)
  - Virtual machines that can be addressed[18] as if they are a separate physical machine should be counted as separate assets,[19] including dynamic and on demand virtual environments

[16] See 44 USC 3554(a)(1)(A)), NIST SP 800-171
[17] 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.
[18] "Addressable" means by IP address or any other method to communicate to the network.
[19] 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.

- Mobile devices:
  - Smartphone
  - Tablets
  - Pagers
- Networking devices:[20]
  - Modems/routers/switches
  - Gateways, bridges, wireless access points
  - Firewalls
  - Intrusion detection/prevention systems
  - Network address translators (NAT devices)
  - Hybrids of these types (e.g., NAT router)
  - Load balancers
  - Encryptors/decryptors
  - VPN
  - Alarms and physical access control devices
  - PKI infrastructure[21]
  - 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.[22] 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).

[20] 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.
[21] PKI assets should be counted as constituent assets on networks in which they reside.
[22] 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.

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.

Local system account
A predefined local account used by service control manager that has extensive privileges on a local system.[23]

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.

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. [24]

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)

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

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).

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.

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 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).