FY 2017 CIO FISMA Metrics

Version 1.00
1 October 2016

This page is intentionally left blank

Table of Contents

GENERAL INSTRUCTIONS

Responsibilities

The head of each Federal agency is responsible for providing 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, as described in the Federal Information Security Modernization Act (FISMA) of 2014 (PL 113-283, 44 USC 3554). Additionally, agency heads are responsible for reporting on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise.

Overview and Purpose

The FY 2017 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. Conversely, 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.

As with the FY 2016 FISMA Metrics, the FY 2017 FISMA metrics are organized 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 *Guide for Applying the Risk Management Framework to Federal Information Systems*[1] 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 2017 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.

Certain high-priority metrics represent the Administration's Cybersecurity Cross Agency Priority (CAP) goals, and they are identified throughout this document as "CAP." The 24 Chief Financial Officer (CFO) Act agencies must report on the status of these metrics on a quarterly basis, at a minimum, and OMB will publish reports on the progress of these metrics in quarterly Cybersecurity CAP Goal Report on Performance.gov. Agencies should provide explanatory

[1] NIST SP 800-37 Rev 1, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.

language for any metric that does not meet established CAP Goal targets (Appendix B). Additionally, in a change from previous years, OMB and DHS removed the designation of "Base" as CFO Act agencies are now expected to report on all metrics contained in this document on a quarterly basis, at a minimum, in accordance with the guidance established in M-17-XX. OMB may also require CFO Act agencies to report on their performance on a more frequent basis, and will provide guidance to those agencies outside of this reporting process.

The expected level of performance for all non-CAP metrics is defined 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). Federal agencies (including independent and small agencies) should report on the status of all metrics as often as needed to ensure that agency leadership has useful, up-to-date information on the level of performance and existing gaps in their cybersecurity posture; at a minimum, CFO Act agencies must provide updates of their progress on a quarterly basis.

1. IDENTIFY

The goal of the Identify metrics section is to assist agencies with their inventory of government furnished equipment (GFE) and other hardware and software systems and assets, which are connected 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.) Answer in Table 1.

	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		
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]												

Table 1: Metrics 1.1.1. – 1.1.4.

1.2. Number of the organization's hardware assets connected to the organization's unclassified network(s). (Note: 1.2. is the sum of 1.2.1. through 1.2.4.) (CAP)

1.2.1. Number of GFE endpoints connected to the organization's unclassified network(s).

1.2.2. Number of GFE mobile assets connected to the organization's unclassified network(s).[2]

1.2.3. Number of GFE networking devices connected to the organization's unclassified network(s).

1.2.4. Number of other GFE input/output devices connected to the organization's unclassified network(s).

1.3. Number of non-GFE hardware assets that are assigned an IP address owned or used by the Agency.

[2] Mobile devices that receive Federal email are considered to be connected.

1.4. Number of GFE hardware assets (from 1.2.) covered by an automatic hardware asset inventory capability (e.g. scans/device discovery processes) at the enterprise-level. (CAP)

1.5. Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) covered by an automated software asset inventory capability at the enterprise-level. (CAP)

For each of the following objectives or outcomes provide key completed activities and key planned activities on a quarterly basis.

Please follow the structure provided in Appendix A for addressing the following:

1.6. Date of issuance of policy empowering incident commanders to direct and manage cybersecurity incidents.

1.7. All contracts with sensitive information contain clauses on the protection/detection/reporting of information, in accordance with OMB guidance.

1.8. Review of contracts with sensitive information, including non-cybersecurity-related contracts, is completed (interim milestone: review of key prioritized contracts with sensitive information is completed).

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. Percent (%) of the organization's unclassified network(s) covered by a capability that blocks unauthorized devices from connecting.

2.2. Percent (%) of the organization's unclassified network(s) assessed for vulnerabilities using Security Content Automation Protocol (SCAP) validated products.[3] (CAP)

2.3. Please complete Table 2. Future configurations will be added as needed.

List of top U.S. Government Operating Systems.	2.3.1. Number of hardware assets with each OS.	2.3.2. The common security configuration baseline for each OS listed. (e.g., USGCB)	2.3.3. Number of assets in 2.3.1 covered by auditing for compliance with 2.3.2. (CAP)
Windows 10.x			
Windows 8.x			
Windows 7.x			
Windows Vista			
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			

Table 2: Metrics 2.3.1. – 2.3.3.

[3] Credentialed scans are only required for assets that recognize credentials. For other assets (e.g., printers), agencies should include the percentage of these assets that are assessed for vulnerabilities with SCAP-validated products.

Unprivileged Network Users

2.4. Number of users with unprivileged network accounts.[4] (Exclude privileged network accounts and non-user accounts.)

2.4.1. Number of users (from 2.4.) technologically required to log onto the network with a two-factor PIV card[5] or other NIST Level of Assurance (LOA) 4 credential.[6] (CAP)

2.4.2. Number of users (from 2.4.) allowed to use username and password as their primary method for network authentication. (CAP)

Privileged Network Users

2.5. Number of users with privileged network accounts. (Exclude unprivileged network accounts and non-user accounts.)

2.5.1. Number of users (from 2.5.) technologically required to log onto the network with a two-factor PIV card[7] or other NIST LOA 4 credential. (CAP)

2.5.2. Number of users (from 2.5.) allowed to use username and password as their primary method for network authentication. (CAP)

Network Accounts

2.6. Number of unprivileged network accounts assigned[8] to users. (Exclude privileged network accounts and non-user accounts.)

2.6.1. Number of unprivileged shared network accounts. (Exclude privileged network accounts and non-user accounts.)

2.6.2. Number of individual users assigned to unprivileged shared network accounts (from 2.6.1).

2.7. Number of privileged network accounts assigned to users. (Exclude unprivileged network accounts and non-user accounts.)

2.7.1. Number of privileged shared network accounts. (Exclude privileged network accounts for single users and non-user accounts.)

---

[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 card 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 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.
[7] For a person with one or more privileged network accounts, the person should be counted in the total only if a two-factor PIV card is necessary to authenticate to all network accounts. The enforcement of authentication may be accomplished via either user based or machine based configuration settings.
[8] An unprivileged network account is any account that is not a privileged network account.

2.7.2. Number of individual users assigned to privileged shared network accounts (from 2.7.1).

2.8. Number of non-user privileged network accounts. (Exclude unprivileged network accounts and privileged network accounts assigned to a user.)

Least Privilege

2.9. Number of privileged network users[9] (from 2.5.) that had their privileges reviewed at least once in the previous quarter (please also update the fiscal year total).

2.10. Number of privileged network users (from 2.5.) that had their privileges adjusted or terminated after a review in the previous quarter (please also update the fiscal year total).

2.11. Number of users with privileged local system accounts.

2.12. Number of users with privileged local system accounts (from 2.11.) technologically required to log onto the system with a two-factor PIV card or other NIST LOA 4 credential.[10]

2.13. Average time (in days) to revoke role-based privileges from Federal employees following the termination of their employment with the agency.

2.14. Average time (in days) to revoke role-based privileges from contractors following the termination of their employment at the agency.

2.15. Average time (in days) to revoke role-based credentials from all other credential holders following the end of their association with the agency.

Physical Access Control Systems

2.16. Percent (%) of agency's operational Physical Access Control Systems (PACS) that comply with procurement requirements for purchasing products and services from the FIPS 201 Approved Products List maintained by General Services Administration (GSA) (per OMB M-06-18).

2.17. Percent (%) of agency's operational PACS that electronically accept and authenticate internal users' PIV credentials for routine access in accordance with NIST standards and guidelines (e.g., FIPS 201-2 and NIST SP 800-116).

---

[9] If the organization conducts its review of network accounts with elevated privileges, rather than of privileged network users, then count the privileged network users as reviewed if any of their network accounts with elevated privileges were reviewed.

[10] For a person with one or more privileged local system accounts, the person should be counted in the total only if a two-factor PIV card is necessary to authenticate for all system access. The enforcement of authentication must be accomplished via machine-based configuration settings.

Data Protection and Remote Access

2.18. Number of systems (from 1.1.) that require all users (100% privileged and 100% unprivileged) to authenticate using a two-factor PIV card or other NIST LOA 4 credential.

2.19. Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) with data encrypted at rest (FIPS 140-2).[11]

2.20. For the remote access connection methods identified in Table 3, report the percentage that have each of the following properties:

Connection Method Type	VPN	VDI/ RDP	Dial up or other (without VPN)
2.20.1. Percent (%) utilizing FIPS 140-2 validated cryptographic modules.	% or NA	% or NA	
2.20.2. 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	
2.20.3. 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
2.20.4. Percent (%) authorizing the use of split tunneling and/or dual-connected remote hosts between trusted entities.	% or NA		% or NA

Table 3: Metrics 2.20.1. – 2.20.4.

Security Training

2.21. Percent (%) of users that successfully completed annual Cybersecurity Awareness and Training (CSAT) in the previous quarter (please also update the fiscal year total).

2.21.1. Percent (%) of new users who satisfactorily completed CSAT before being granted network access or within an organizationally defined time limit.

2.22. Number of users (from 2.4. & 2.5.) that have significant security responsibilities.[12]

[11] Per *NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices*, data at rest refers to data storage, as opposed to data transmission.

[12] Those with significant security responsibilities include administrators and users with privileged network accounts and those that affect security. Those with budget and staffing responsibilities should not be considered as having significant security responsibilities.

2.22.1. Number of users (from 2.22.) that have successfully completed role-based security training within the organization's defined periodicity.

2.23. Number of users that participated in exercises focusing on phishing that are designed to increase awareness and/or measure effectiveness of training (e.g. organization conducts spoofed phishing emails, clicking links leading to phishing information page) in the previous quarter (please also update the fiscal year total).

2.23.1. Number of users (from 2.23.) that successfully passed the exercise.

2.23.2. Number of users (from 2.23.) that identified[13] and reported the phishing exercise to the appropriate agency cybersecurity resource.

Trusted Internet Connection (TIC) Boundary Protection

The purpose of the TIC program is to ensure that agencies are progressing in adopting TIC to protect their networks. The goals of the TIC Program are to inventory Federal external connections, meet the defined TIC security controls and route all agency traffic through defined access points.[14] Agencies that operate their own TIC Access Points are referred to as TIC Access Providers (TICAPs). Agencies that need to acquire services are referred as Seeking Service Agencies (SSAs). (Smaller agencies are encouraged to seek Managed Trusted Internet Protocol Services (MTIPS) services through the GSA Networx contract[15]).

2.24. **For agencies that are TIC Access Providers (TICAP)**: In the below table provide the TIC 2.0 critical capabilities that have been identified as NOT MET during your agency's last TIC Compliance Validation (TCV) assessment.

Missing Critical Capabilities	Reason Not Met (drop down menu)	Expected Implementation Date	Comments
Ex. TM.COM.01	Policy	1/6/18	

Table 4: Metric 2.24.[16]

2.25. **For agencies that obtain TIC services through a provider (usually via an MTIPS provider)**:

2.25.1. Identify all of the TIC 2.0 critical capabilities enabled by your provider.

[13] Identification can be through general awareness or after clicking/opening the attempt.
[14] Trusted Internet Connection requirements are highlighted by:
- OMB M-08-05 Implementation of Trusted Internet Connections (TIC)
- OMB M-08-16 Guidance for Trusted Internet Connection Statement of Capability Form (SOC)
- OMB M-08-27 Guidance for Trusted Internet Connection (TIC) Compliance
- OMB M-09-32 Update on the Trusted Internet Connections Initiative

[15] GSA Networx is the government's network solutions contract for Federal agencies.
[16] This section will be pre-populated from the last TCV assessment.

2.25.2. Identify all of the TIC 2.0 critical capabilities that your agency manages internally. (These are typically in place because they are not enabled by your provider)

2.25.3. Identify all recommended capabilities[17] that your agency provides internally or via your provider (in addition to those identified in 2.25.1. and 2.25.2.).

Technical Information: TIC Access Points (excluding MTIPS)

2.26. Please use the table below to report the following information about your current and planned internet connections.

2.26.1. Current Access Points						
TIC Access Point Name	**TIC Access Point Location**	**Internet Service Provider**	**Internet Circuit Size (Mbps)**	**Capacity Rate (Mbps)**	**EINSTEIN 2 Monitored**	**ATO Date**
Add rows as necessary						
Total			*(Calculated)*	*(Calculated)*		
2.26.2. Planned Access Points (estimated)						
TIC Access Point Name	**TIC Access Point Location**	**Internet Service Provider**	**Internet Circuit Size (Mbps)**	**Capacity Rate (Mbps)**	**EINSTEIN 2 Monitored**	**ATO Date**
Add rows as necessary						
Total			*(Calculated)*	*(Calculated)*		

Table 5: Metrics 2.26.1. - 2.26.2.

Technical Information: Managed Trusted Internet Protocol Services (MTIPS) Connections

2.27. Please report the current and planned MTIPS connections for your agency.

2.27.1 Current MTIPS Access Points			
MTIPS Provider	**Capacity Rate (in Mbps)**	**Description**	**ATO Date**
Add rows as necessary			
Total	*(Calculated)*		
2.27.2 Planned MTIPS Access Points (estimated)			
MTIPS Provider	**Capacity Rate (in Mbps)**	**Description**	**ATO Date**
Add rows as necessary			
Total	*(Calculated)*		

[17] TIC Security guide identifies 14 recommended capabilities. These are capabilities, which are not required, but are optional for the agency to support.

Table 6: Metrics 2.27.1. - 2.27.2.

Technical Information: Internet

2.28. Please provide future growth and capacity of your internet connections.

Month/Year	Aggregate Internet Capacity (Mbps)
Oct 16	(This number will be pre-populated from the 'Capacity Rate' entered in the above Section)
Oct 17	
Oct 18	

Table 7: Metric 2.28.

Unmonitored Connections

2.29. Report the type of .gov user Internet traffic not going through the TIC (e.g., mobile government users to cloud assets, R&D networks, human resources applications accessible through the Internet, etc.):

****Example 1:** Agency mobile users at an Internet cafe accessing their email/office automation that resides in a Microsoft Office 365 cloud instance directly (without routing through the agency TIC Access Points.)

****Example 2:** Users on an agency network that is not the General Support System (e.g., guest Internet café at a government site, development network with sensitive data, etc.) accessing Internet web sites not directed through the agency's TIC Access Points.

****Example 3:** Agency contractor networks containing government data with direct Internet connections that do not pass through agency's TIC Access Points.

Technical Information: Extranet

2.30. Please report your current and planned extranet connections (consolidated and non-consolidated) in the table below.

2.30.1 Extranet traverses (aka consolidated) through an agency MTIPS/TICAP connection		
Month and Year	**Number of Circuits**	**Total Extranet Capacity (Mbps)**
Oct 16		
Oct 17		
Oct 18		
2.30.2 Extranet by-passes (aka non-consolidated) the agency's MTIPS/TICAP connection(s)		
Month and Year	**Number of Circuits**	**Total Extranet Capacity (Mbps)**
Oct 16		
Oct 17		

Oct 18		

2.30.3 Extranet by-passes (aka non-consolidated) the agency's MTIPS/TICAP connection(s)			
Connection Location	**Provider**	**Circuit Size (in Mbps)**	**Capacity/Rate Limiter (in Mbps)**
1 <site name> <city, State>		(example: DS3, T1)	
2			
3			
Add rows as necessary			

Table 8: Metrics 2.30.1. - 2.30.3.

Technical Information: Cloud Services

2.31. Report what types of Cloud Services your agency is using. Document your cloud service provider and service you are receiving (e.g., mail, database, etc.) in the table below.

Cloud Service Provider	Cloud Service Offering	Agency ATO Date	Sub-Agency	Service	Service Type (Drop Down)
Ex. Microsoft	Office 365	2/21/15	Storage	Email and collaboration solutions	IaaS
Add rows as necessary					

Table 9: Metric 2.31.

Data in Motion[18]

2.32. Percent (%) of all external and internal websites and services under the control of the agency or operated on the agency's behalf that are accessible through a secure connection (HTTPS-only, with HSTS), per OMB Memorandum M-15-13.

2.32.1. Percent (%) of external-facing websites and services under the control of the agency or operated on the agency's behalf that are accessible only through a secure connection (i.e., HTTPS-only, with HTTP Strict Transport Security (HSTS).

2.32.2. Percent (%) of internal websites and services under the control of the agency or operated on the agency's behalf that are accessible through a secure connection (HTTPS-only, with HSTS).

2.33. Percent (%) of all new acquisitions within the past twelve months that include the creation or maintenance of external and/or internal websites and services which mandate the use of HTTPS-only, with HSTS.

[18] Per NIST, data in motion is data that moves through the network to the outside world via email, instant messaging, or other communication mechanisms.

For each of the following objectives or outcomes provide key completed activities and key planned activities on a quarterly basis.

Please follow the structure provided in Appendix A for addressing the following:

2.34. Dates of the most recent test phishing exercises and results of the exercise.

2.35. Date of the most recent assessment of the agency's Insider Threat Program, per Executive Order 13587, by the National Insider Threat Task Force and results of the assessment.

2.36. Date of issuance of an enterprise-level policy for destroying media containing sensitive information in line with the specifications outlined in NIST SP 800-88 Revision 1.

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.

Anti-Phishing Defense

3.1. Percent (%) of incoming email traffic passing through anti-phishing and anti-spam filtration at the outermost border mail agent or server. (CAP)

3.2. Percent (%) of incoming email traffic analyzed using sender authentication protocols (e.g., DKIM, DMARC, VBR, SPF, iprev). (CAP)

3.3. Percent (%) of incoming email traffic analyzed using a reputation filter (to perform threat assessment of sender). (CAP)

3.4. Percent (%) of incoming email traffic analyzed for detection of clickable URLs, embedded content, and attachments. (CAP)

3.5. Percent (%) of incoming email traffic analyzed for suspicious or potentially nefarious attachments and opened in a sandboxed environment or detonation chamber. (CAP)

3.6. Percent (%) of outgoing email traffic that enables the recipients to verify the originator using sender authentication protocols (e.g., DKIM, DMARC, VBR, SPF, iprev). (CAP)

Malware Defense

3.7. Number of GFE endpoints (from 1.2.1.) covered by an intrusion prevention system. (CAP)

3.8. Number of GFE endpoints (from 1.2.1.) covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information. (CAP)

3.9. Number of GFE endpoints (from 1.2.1.) covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar). (CAP)

3.10. Number of GFE endpoints (from 1.2.1.) protected by a browser-based (e.g., Microsoft SmartScreen Filter, Microsoft Phishing Filter, etc.) or enterprise-based tool to block known phishing websites and IP addresses. (CAP)

3.11. Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) authorized for remote access connection to the unclassified network.

3.11.1. Number of assets (from 3.11.) scanned for malware prior to an authorized remote access connection to the unclassified network. (CAP)

Other Defenses (capabilities beyond those provided by traditional Anti-Phishing & Malware defenses)

3.12. Percent (%) of users with privileged network accounts (from 2.5.) that have a technical control limiting access to only trusted sites. (CAP)

3.13. Percent (%) of inbound network traffic that passes through a web content filter, which provides anti-phishing, anti-malware, and blocking of malicious websites (e.g., fake software updates, fake antivirus offers, and phishing offers). (CAP)

3.14. Percent (%) of outbound communications traffic checked at the external boundaries to detect encrypted exfiltration of information (i.e. agency's capability to decrypt/interrogate and re-encrypt). (CAP)

3.15. Percent (%) of email messages processed by systems that quarantine or otherwise block suspected malicious traffic. (CAP)

Network Defense

3.16. Percent (%) of the organization's unclassified network that has implemented a technology solution to detect and alert on the connection of unauthorized hardware assets. (CAP)

3.16.1. Mean time to detect a new device (time between scans in 3.16.).

3.17. Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) covered by a software asset management capability to detect, alert, and/or block unauthorized software from executing (e.g., certificate, path, hash value, services, and behavior based whitelisting solutions). (CAP)

For each of the following objectives or outcomes provide key completed activities and key planned activities on a quarterly basis.

Please follow the instruction in Appendix A for addressing the following:

3.18. Date of the most recent test exfiltration attempt and results of the exercise.

3.19. Attempts to access large volumes of data are detected and investigated.

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 the last update to the Incident Response Plan.

4.2. Number of computer security incidents reported to agency Security Operations Centers or other appropriate agency resource this quarter (please also update the fiscal year total).

4.2.1. Number of computer security incidents reported to US-CERT this quarter (please also update the fiscal year total).

For each of the following objectives or outcomes provide key completed activities and key planned activities on a quarterly basis.

Please follow the structure provided in Appendix A for addressing the following:

4.3. Date of the last test of the Worst-case Incident Response Plan (per NIST SP 800-83) and date of most recent update to the plan.

4.4. Established partnership for surge resources with other agencies and details of the special capabilities that these surge partners will provide.

4.5. Verified roles and responsibilities prior to or during incident response testing.

4.6. Incident Response Plan is at the enterprise level, and developed and tested at least twice annually (i.e., twice over a 365-day period).

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 the last update to the Incident Recovery Plan.

5.2. Date of the last update to the Disaster Recovery Plan.

5.3. Percent (%) of public/internal notifications that were conducted in accordance with relevant statue, OMB policy, or agency policies.

For each of the following objectives or outcomes provide key completed activities and key planned activities on a quarterly basis.

Please follow the structure provided in Appendix A for addressing the following:

5.4. Disaster Recovery plans (per NIST SP 800-34) covers human threat sources, including ones impacting electronic information or resulting in physical data loss.

5.5. Business Continuity plans (per NIST SP 800-34) are in place and fully tested for all levels of relevant cybersecurity related incidents.

5.6. An Incident Recovery Plan (per NIST Cybersecurity Framework) is at the enterprise level and developed, updated, and tested at least annually.

5.7. A Disaster Recovery Plan (per NIST Cybersecurity Framework) is at the enterprise level and developed, updated, and tested at least annually.

5.8. Policy is in place regarding timelines for public and internal incident notifications (per NIST SP 800-122).

5.9. Metrics tracking for public and internal notifications conducted in accordance with agency policies are in-place.

5.10. Agency has a credit repair contract in place, or demonstrates that it is ready to leverage a contract by having assessed the scope, cost, and time to execute such a contract.

5.11. Agency has a credit monitoring contract, such as the BPA provided by GSA, in place, or demonstrates that it is ready to leverage a contract by having assessed the scope, cost, and time to execute such a contract.

APPENDIX A: REPORTING STRUCTURE FOR KEY ACTIVITIES

Appendix A provides structure for reporting completed activities or milestones, and planned activities or milestones for accomplishing a specific objective or outcome. These will be used to determine progress.

For completed activities or milestones:

Completed key activities or milestones		
Key Activities of Milestones	**Target Date** (previously reported)	**Completed Date**
Add rows as necessary		

For planned key activities or milestones.[19]

Planned key activities or milestones	
Planned Activities of Milestones	**Target Date**
Add rows as necessary	

[19] Agencies can also provide planned activities for any of the FISMA metrics where new best practices may be beneficial government-wide.

APPENDIX B: SUMMARY OF FISMA CAP GOAL TARGETS & METHODOLOGY

Appendix B 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 2017 Annual FISMA CIO Metrics**	**FY 2016 Annual FISMA CIO Metrics**	**Agency Calculation**
Information Security Continuous Monitoring (ISCM)				
Hardware Asset Management	≥ 95%		1.4, 3.16	Both results must be greater than or equal to target
Software Asset Management	≥ 95%		1.5, 3.17	Both results must be greater than or equal to target
Vulnerability and Weakness Management	≥ 95%		2.2	Result must be greater than or equal to target
Secure Configuration Management	≥ 95%		2.3.4	Result must be greater than or equal to target
Identity and Credential Access Management (ICAM)				
Unprivileged Network Users	≥ 85%		2.4.1	Result must be greater than or equal to target
Privileged Network Users	100%		2.5.1	Result must equal target
Anti-Phishing and Malware Defense				
Anti-Phishing Defense	≥ 90%		2.19.1, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6	Top 5 results must be greater than or equal to target
Malware Defense	≥ 90%		3.7, 3.8, 3.9, 3.10, 3.11.1	Top 3 results must be greater than or equal to target
Other Defenses	≥ 90%		3.12, 3.13, 3.14, 3.15	Top 2 results must be greater than or equal to target

Table 10: Summary of CAP Goal Target & Methodology

APPENDIX C: DEFINITIONS

Capacity rate
Capacity rate is the max rate that the circuit can burst to and not the CIR (Committed Information Rate). For example, an Agency may have a 1000 Mbps link (1 Gbps), with a contracted rate of 400 Mbps, and a burst of 100 Mbps. In this case, the "Capacity Rate" would equal 500 Mbps. The Capacity Rate is also known as the "Peak Information Rate."

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.

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.

Extranet
Network connections between Federal networks and non-Federal partners.

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

[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

- 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 infrastructure[24]
- 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 (per 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.

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://www.gsa.gov/portal/category/102371.

[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.

[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.

Internet circuit size
Internet Circuit Size is the 'link speed' of the connection. For example, an agency has a 1000 Mbps link (1 Gbps), with a CIR (Committed Information Rate) of 400 Mbps and a burst of 100 Mbps. In this case, the Internet Circuit Size would be recorded as 1000 Mbps.

Managed Trusted Internet Protocol Services (MTIPS)
Managed compliant TIC solutions sold by a NETWORX vendor to a Federal Government agency.

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 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).

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.

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.

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 Table 3.

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

Secondary network
Networks where agencies are leveraging MTIPS providers to provide services to sub-components or networks other than their primary network. These non-primary connections can be considered secondary networks. Examples of secondary networks include: connections that support a specific mission or component, R&D networks, OIG networks, guest wireless, etc.

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)
- Vouch by Reference (VBR)
- Sender Policy Framework (SPF)
- IP Reverse (iprev)

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.

TIC 2.0 capabilities
A body of 60 critical capabilities that were collaboratively developed to improve upon the baseline security requirements in TIC Reference Architecture v2.0. These are available via the MAX Federal Community (https://community.max.gov/x/I4R_Ew).

Unclassified information system(s)
Information system(s) processing, storing, or transmitting information that does not require safeguarding or dissemination controls pursuant to Executive Order (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 2016, these components are limited to endpoints, mobile assets, network devices, and input/output assets as defined under hardware assets.

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.)