FY15 CIO Annual FISMA Metrics

Version 1.2

30 July, 2015

Document History

Version	Date	Comments	Author	Sec/Page
1.0	12 September 2014	Initial release of FY15 CIO annual FISMA metrics	DHS FNR	All
1.1	10 October 2014	Added definition of network fabric	DHS FNR	Appendix A
1.2	30 July 2015	Added new Appendices A and B, updated footnotes, and formatting changes throughout	DHS FNR	All

Table of Contents

GENERAL INSTRUCTIONS

Responsibilities

Organization[1] heads are responsible for complying with the Federal Information Security Modernization Act of 2014 (FISMA) and have full authority to require reporting by their components that form their enterprise.

Fiscal Year (FY) 15 FISMA Metric Development Process

While we move the Federal government toward Information Security Continuous Monitoring (ISCM) solutions, such as Continuous Diagnostics and Mitigation (CDM), it is important that we take appropriate actions to continue making the current direct-entry reporting methods less burdensome to Departments and Agencies (D/As) and to improve the quality of the data being reported. The current FISMA Chief Information Officer (CIO) metrics have been improved to provide more value to congressional and executive audiences, as well as, individual D/As.

In coordination with the Office of Management and Budget (OMB) and the National Security Council (NSC) staff, the Federal Network Resilience (FNR) Division of the Department of Homeland Security (DHS) is developing long-term solutions to automate the CIO reporting process by leveraging the benefits of emerging continuous monitoring capabilities and other data collection mechanisms. However, FNR knows there are opportunities in the short-term to improve the FISMA cybersecurity metrics. This year DHS/FNR did so by facilitating an online collaborative effort incorporating the input of more than 100 cybersecurity professionals from over 24 D/As utilizing an Agile methodology. The goal of this effort was to improve the validity, quality, and efficiency of cybersecurity governance data and collection efforts. The participating cybersecurity professional made over 200 recommendations, and the DHS/FNR cybersecurity experts incorporated these recommendations into this set of FY 2015 CIO Annual FISMA Metrics.

Expected Levels of Performance

Cross-Agency Priorities (CAP)

The expected levels of performance for CAP FISMA metrics are based on review and input from multiple cybersecurity experts as well as threat information from public, private, and intelligence sources.[2] Q1 and Q2 FY15 were used to establish a baseline to generate a scoring methodology for the CAP goals (See Appendix B: Summary of FISMA CAP Goal Targets and Methodology). The Administration's Priority (AP) cybersecurity capabilities are currently:

- Information Security Continuous Monitoring—Provide ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity: posture, hygiene, and operational readiness.
- Identity Credential and Access Management—Implement a set of capabilities that ensure users must authenticate to information technology resources and have access to only those resources that are required for their job function.

[1] The term "organization" refers to each Federal D/A that is a reporting unit under CyberScope.
[2] See Cross-Agency Priority Goals for further details.

- Anti-phishing and Malware Defense—Implement technologies, processes and training that reduce the risk of malware introduced through email and malicious or compromised web sites.

Key FISMA Metrics (KFM)

The expected level of performance for these metrics is defined as "adequate security," which means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of government information. This includes assuring that systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.[3]

In compliance with OMB FISMA guidance (M-11-33, FAQ 15), the D/A head is responsible for determining the acceptable level of risk, with input from system owners, program officials, and CIOs.

Baseline Questions (Base)

These questions establish current performance against which future performance may be measured. There is no expected level of performance for baseline questions. Some baseline questions are also intended to determine whether such future performance measures are needed. Offices of the Inspector General (OIG) should not assume that these questions define any specific organizational performance standard for 2015.

National Institute of Standards and Technology Special Publication (NIST SP) 800 Revisions

For legacy information systems, D/As are expected to be in compliance with NIST guidelines within one year of the publication date. D/As must become compliant with any new or updated materials in revised NIST guidelines within one year of the revision. For information systems under development or for legacy systems undergoing significant changes, D/As are expected to be in compliance with the NIST publications immediately upon deployment of the information system. Each D/A should consider its ability to meet this requirement when developing the Plan of Action and Milestones (POA&M).

Federal Information Processing Standards (FIPS) Versions

References in this document to FIPS Standards refer to the latest (non-draft) published version.

[3] Office of Management and Budget (OMB) Circular A-130, Appendix III, definitions.

1. SYSTEM INVENTORY

Purpose and Use

- System inventory is a basic tool to identify systems (and their boundaries).
- A key goal of this process is to ensure that systems are acquired/engineered, operated, and maintained to provide minimal acceptable security. This includes a risk assessment and authorization to operate before becoming operational.[4]

1.1. For each FIPS 199 impact level, what is the total 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 (Base)			1.1.2. Contractor-Operated Systems (Base)			1.1.3. Systems (from 1.1.1 and 1.1.2) with Security ATO (signed, in-scope) (KFM)		
FIPS 199 Category	**H**	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**
Reporting Organization 1									
Reporting Organization 2									
[Add rows as needed for organization]									

Table 1: Metric 1.1.1.–1.1.3.

1.2. How many endpoints belong to systems without a valid ATO? (KFM)

1.3. How many public facing systems are without a valid ATO? (KFM)

[4] Departments and agencies who report systems are expected to follow the Risk Management Framework (RMF), to include guidance on security plans and risk assessments, as outlined in NIST SP 800-37 rev 1 and NIST SP 800-137.

2. INFORMATION SECURITY CONTINUOUS MONITORING

Purpose and Use

- OMB M-14-03 directs D/As to implement continuous monitoring of security controls as part of a phased approach through FY 2017.
- At the level of the Federal enterprise, the current metrics aim to provide situational awareness as to where agencies stand with implementing and operating continuous monitoring as it is envisioned by NIST SP 800-137, DHS Continuous Diagnostics and Mitigation (CDM), and the Information Security Continuous Monitoring (ISCM) Concept of Operations (ConOps).
- The Joint Continuous Monitoring Working Group (JCMWG) recommends that asset management is one of the first areas where continuous monitoring needs to be developed. Organizations must first know about devices and software (both authorized/managed and unauthorized/unmanaged) before they can manage the devices/software for configuration and vulnerabilities.
- A key goal of ISCM is to make hardware assets harder to exploit through hardware asset management, software asset management, secure configuration management, and vulnerability management.

Hardware Asset Management

2.1. What is the total number of the organization's hardware assets connected to the organization's unclassified[5] network(s)?[6] (Base)

2.1.1. Percent (%) of assets from 2.1 that store (e.g., on an endpoint or maintained as a record in an external asset management database) meta-data (e.g. system association, owner, location)? (Base)

2.1.2. What is the total number of endpoints connected to the organization's unclassified network(s)? (Base)

2.2. Percent (%) of the organization's network fabric covered by a capability to detect and alert on the addition of unauthorized hardware assets onto the organization's network. (AP)

2.3. Percent (%) of the organization's network fabric covered by an automatic capability (scans/device discovery processes) that provides enterprise-level visibility into the current state of all hardware assets. (AP)

2.4. What is the mean time[7] to detect a new device (time between scans in 2.2)? (AP)

2.5. Percent (%) of the organization's registered network fabric covered by a Network Access Control switching technology that blocks unauthorized devices. (Base)

[5] "Unclassified" refers to low impact (non-sensitive) and sensitive but unclassified (SBU) data.
[6] Unless specified otherwise in a footnote, add numbers across networks and organizational components to get the reportable result.
[7] Mean time is measured in calendar days.

Software Asset Management

2.6. Percent (%) of endpoints from 2.1.2 covered by an automated software asset inventory capability to scan the current state of installed software (e.g., .bat, .exe, .dll). (AP)

2.7. Percent (%) of endpoints from 2.1.2 covered by a desired-state software asset management capability to detect and block unauthorized software from executing (e.g., AppLocker, certificate, path, hash value, services, and behavior based whitelisting solutions).[8] (AP)

2.8. How many major application databases[9] does the organization maintain? (Base)

2.9. Percent (%) of the organization's network fabric that undergoes periodic discovery scanning specifically for the purpose of identifying and enumerating databases. (KFM)

[8] This may include software whitelisting tools that identify executable software by a digital fingerprint and selectively block these. It might also include sandboxing of mobile code to determine before execution whether to allow it to run, where static files do not allow whitelisting. In general, any method included should be able to block zero-day and Advanced Persistent Threats (APT).

[9] Major application databases are those supporting a FIPS-199 'high' impact level, unclassified, operational information systems from questions 1.1.1 and 1.1.2.

Secure Configuration Management (SecCM)

2.10. Please complete Table 2. Future configurations will be added as needed. Data calls for layer 2, layer 3, mobile, printers, or other devices or operating systems will be used as needed.

List of top U.S. Government Operating Systems, as reported in SCAP feeds.	2.10.1 What is the number of hardware assets with each OS? (Base)	2.10.2 What is the common security configuration baseline for each OS listed? (Base) (e.g., USGCB)	2.10.3 How many configuration exceptions are granted by the enterprise? (Base)	2.10.4 What is organization's enterprise policy for maximum audit interval (target)? (Base)	2.10.5 What is organization's enterprise average audit interval (actual)? (AP)	2.10.6 Percent (%) of assets in 2.10.1 covered by the auditing activities described in 2.10.4 and 2.10.5. (AP)
Windows 8.x						
Windows 7.x						
Windows Vista						
Windows Unsupported (include XP)						
Windows Server 2003						
Windows Server 2008						
Windows Server 2012						
Linux (all versions)						
Unix/Solaris (all versions)						
Mac OS X						

Table 2: Metric 2.10.1–2.10.6.

Vulnerability and Weakness Management

2.11. Percent (%) of hardware assets listed in 2.1 assessed using credentialed scans with Security Content Automation Protocol (SCAP) validated vulnerability tools.[10] (AP)

2.12. What is the mean time[11] between vulnerability scans? (AP)

2.13. Percent (%) of the databases in 2.8 that undergo periodic vulnerability scanning with a special purpose database vulnerability scanner. (KFM)

2.14. What is the mean time[12] to mitigate for high[13] findings? (AP)

[10] Vulnerability scanning tools are SCAP validated – assets are not.
[11] Mean time is measured in calendar days.
[12] Mean time is measured in calendar days.
[13] The National Vulnerability Database (NVD) provides severity rankings of "Low" "Medium" and "High" for all Common Vulnerabilities and Exposures (CVE) in the database. The NVD is accessible at http://nvd.nist.gov.

3. IDENTITY CREDENTIAL AND ACCESS MANAGEMENT

Purpose and Use

- Strong information system and physical access authentication requires multiple factors to securely authenticate a user. A single-factor authentication mechanism, such as a username and password, is insufficient to block even basic attackers.
- Enhanced identity management solutions also support the adoption of additional non-security benefits, such as single sign-on, more accountable and efficient use of systems, and enhanced identity capabilities through use of electronic signatures for legal and non-repudiation needs.
- A key goal of identity credential and access management (ICAM) is to strike a proper balance between data access "need-to-know" and "need-to-share" making sure that access rights are given only to the intended individuals and/or processes.[14]
- For more information regarding Personal Identity Verification (PIV) eligibility, please see the OPM's Final Credentialing Standards for Issuing Personal Identity Verification Cards under Homeland Security Presidential Directive 12 (HSPD-12) here.

Unprivileged Network Users

3.1. How many users have unprivileged network accounts?[15] (Exclude privileged network accounts and non-user accounts.) (Base)

3.1.1. Percent (%) of users from 3.1 technically required to log onto the network with a two-factor PIV card[16] or NIST Level of Assurance (LOA) 4 credential. [17] (AP)

Privileged Network Users

3.2. How many users have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.) (KFM)

3.2.1. Percent (%) of users from 3.2 technically required to log onto the network with a two-factor PIV card[18] or NIST Level of Assurance (LOA) 4 credential. (AP)

3.3. Percent (%) of privileged network users[19] that had their privileges reviewed this year. (KFM)

3.4. Percent (%) of privileged network users that had their privileges adjusted or terminated after being reviewed this year. (Base)

---

[14] The process to establish an individual's access rights first determines that the individual has a need to know, assigns appropriately restricted access rights, and uses the individual's digital identity to authenticate the individual, then grants access rights.

[15] An unprivileged network account is any account that is not a privileged network account.

[16] For a person with one or more unprivileged network accounts, the person should be counted in the percentage 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.

[17] For additional information, refer to http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.

[18] For a person with one or more privileged network accounts, the person should be counted in the percentage 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.

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

Internal Systems

3.5. Percent (%) of the organization's internal systems[20] configured to require PIV authentication. (KFM)

3.6. Percent (%) of the organization's government service portals (e.g., Max.gov Portal, MyEPP) that enforce PIV authentication for cross-agency federal customers. (If none are provided, answer N/A.) (KFM)

Remote and Mobile Device Access Solutions

3.7. How many users log onto the organization's remote access solution(s)[21] to obtain access to the organization's desktop LAN/WAN resources or services? (Base)

3.7.1. Percent (%) of the users reported in 3.7 required to use two-factor PIV card authentication to remotely log onto the organization's desktop LAN/WAN resources or services.[22] (KFM)

3.8 How many users are enabled to remotely log onto the organization's LAN/WAN resources or services from mobile devices? (Base)

3.8.1. Of the organization's users who remotely access desktop LAN/WAN resources or services from mobile devices, what percent (%) of these users are technically required to use two-factor PIV card authentication to access these resources and services? (KFM)

Physical Access Control Systems

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

3.10. 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). (KFM)

---

[20] Internal systems include those that are accessed by internal organization users, defined for the purpose of this question as Federal employees, contractors, and affiliates, covered under the scope of HSPD-12. System implementations protected by an Identity and Access Management solution that adheres to the principles above are also considered PIV-enabled.

[21] When reporting how many PIV credentials are being used for logical access to systems, agencies should include the following implementations: remote or networked logical access system implementations are PIV-enabled when the Public Key Infrastructure (PKI) certificate presented at authentication is validated (i.e., found to be legitimately issued, unexpired, and unrevoked) under Federal Common Policy as a PIV Authentication Certificate and the corresponding "PIV Authentication Key" on the card correctly responds to the cryptographic challenge in the authentication protocol to gain access. Certificate validation may be performed by an intermediary service such as a Server-based Certificate Validation Protocol (SCVP) server. Revocation checking may be accomplished by 'caching' revocation information from the credential issuer provided the cache is refreshed at least once every 18 hours. Local workstation logical access system implementations are PIV-enabled when the BIO, BIO-A, CHUID, or PIV Authentication credentials and authentication protocols are in conformance with authentication mechanisms defined in FIPS 201 and NIST SP 800-73, digital signatures on data objects used are verified, and certificates used are validated. System implementations protected by an Identity and Access Management solution that adheres to the principles above are also considered PIV-enabled. For additional information, refer to FIPS 201, NIST SP 800-73, and Federal PKI Policy and FICAM Roadmap and Implementation Guidance.

[22] This phrasing is primarily intended to exclude mobile devices as they are covered in a separate metric.

4. ANTI-PHISHING AND MALWARE DEFENSE

Purpose and Use

- Due to the preponderance of phishing attacks and their steadily increasing frequency and sophistication, anti-phishing and malware defense was added as a Cross-Agency Priority (CAP) goal beginning in FY15. United States Computer Emergency Readiness Team (US-CERT) and National Security Agency (NSA) both identified phishing as one of the top threat vectors putting Federal Departments and Agencies at risk.
- Phishing metrics are designed to assess maturity across a variety of anti-phishing techniques, including filtering of emails used to deliver malicious content, network-level defenses, endpoint-level defenses,[23] and training.
- Gateway defenses are the first line of defense in protecting organization networks, and enterprise level solutions are necessary to block/filter the majority of phishing attempts, including web content filtering, mail filtering, and mail verification.
- Phishing attacks seek to convince users to provide information or access needed for an attacker to steal information or compromise a network. It is important for users to understand, be able to identify, and be able to protect themselves from phishing attacks.

4.1. Percent (%) of privileged user accounts that have a technical control preventing internet access. (AP)

4.2. Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments. (AP)

4.3. Percent (%) of hardware assets covered by a host-based intrusion prevention system. (AP)

4.4. Percent (%) of hardware assets covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information. (AP)

4.5. Percent (%) of email attachments opened in sandboxed environment or detonation chamber. (AP)

4.6. Percent (%) of incoming emails using email sender authentication protocols such as DomainKeys Identified Mail (DKIM), Author Domain Signing Practices (ADSP), Domain-based Message Authentication, Reporting & Conformance (DMARC), Vouch by Reference (VBR), or IP Reverse (iprev). (AP)

4.7. Percent (%) of incoming emails scanned using a reputation filter[24] tool to perform threat assessment of email sender. (AP)

4.8. Percent (%) of hardware assets covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar). (AP)

4.9. Percent (%) of inbound email traffic passing through anti-phishing/anti-spam filtration technology at the outermost border Mail Transport Agent or email server. (AP)

---

[23] Endpoint-level defenses provide another layer in a defense-in-depth approach to help mitigate phishing attacks in the event that an attack gets through gateway defenses.

[24] Outer layer of email protection filters potentially malicious email based on sender reputation, sender IP address, or other sender information.

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

4.11. Percent (%) of hardware assets that have implemented a browser-based (e.g., Microsoft Phishing filter) or enterprise-based tool to block known phishing websites and IP addresses. (AP)

4.12. Percent (%) of outbound communications traffic checked at the external boundaries to detect covert exfiltration of information. (AP)

4.13. Percent (%) of sent email that is digitally signed. (AP)

4.14. Percent (%) of email traffic quarantined or otherwise blocked. (AP)

5. DATA PROTECTION

Purpose and Use

- Mobile devices and unencrypted email are primary sources of loss for sensitive data because they move outside the protection of physical and electronic barriers that protect other hardware assets. These devices are also vectors to carry malware back into the organization's networks. The use of encryption of data at rest or in motion is vital to protect that data's confidentiality and integrity.

5.1. What is the estimated number of hardware assets in each of the following mobile and portable asset types, and how many are encrypted? Answer in Table 3.

Mobile and Portable Device Types (each asset should be recorded *no more than once* in each column).	**5.1.1 Estimated number of mobile hardware assets of the types indicated in each row. (Base)**	**5.1.2 Estimated number of assets from 5.1.1 with FIPS 140-2 compliant encryption of data on the device.[25] (KFM)**
Laptop computers and netbooks		
Tablet-type computers		
Smartphones		
Other mobile devices		

Table 3: Metric 5.1a–5.1b

[25] The numbers in 5.1.2 cannot be larger than the numbers in 5.1.1.

6. NETWORK DEFENSE

Purpose and Use

- Attackers exploit boundary systems on internet-accessible demilitarized zone (DMZ) networks (and on internal network boundaries) and then pivot to gain deeper access on internal networks.
- Remote connections allow users to access the network without gaining physical access to its organization's facility and the computers hosted there. However, connections over the internet provide opportunities for compromise of information in transit. Because these connections are beyond physical security controls, they need compensating controls to ensure that only properly identified and authenticated users gain access, and that the connections prevent hijacking by others.

6.1. What is the estimated percent (%) of remote access connections that have each of the following properties:

6.1.1. Percent (%) that utilize FIPS 140-2-validated cryptographic modules. (KFM)

6.1.2. Percent (%) that prohibit split tunneling[26] and/or dual-connected[27] remote hosts where the mobile device has two active connections. (KFM)

6.1.3. Percent (%) configured in accordance with OMB M-07-16 to time-out after 30 minutes of inactivity (or less) and requires re-authentication to reestablish session. (KFM)

6.1.4. Percent (%) scanned for malware upon connection. (AP)

[26] A method that allows a VPN user to access a public network (e.g., the internet) and a local LAN or WAN at the same time, using the same physical network connection. This connection service is usually facilitated through a program such as a VPN client software application.

[27] An environment where the host is connected to more than one network. The connections may be wired or wireless.

7. BOUNDARY PROTECTION

Purpose and Use

- Boundary protection is the monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
- Two goals of boundary protection are to increase Trust Internet Connections (TIC) consolidation and implementation of TIC capabilities.

7.1. Percent (%) of the required TIC 2.0 Capabilities implemented. (KFM)

7.2. Percent (%) of external network traffic to/from the organization's networks that passes through a TIC/MTIPS. (KFM)

7.3. Percent (%) of external network/application interconnections to/from the organization's networks that passes through a TIC/MTIPS. (KFM)

7.4. Percent (%) of public-facing servers[28] use IPv6 (e.g., web servers, email servers, DNS servers, etc.). (Exclude low-impact networks, cloud servers, and Internet Service Provider (ISP) resources unless they require IPv6 to perform their business function.) (KFM)

[28] While the mandate refers to "servers and services," IPv6 addresses apply to hardware assets, not services. To avoid double counting, this question refers to the servers only, both physical and virtual. The servers included should host public-facing services.

8. TRAINING AND EDUCATION

Purpose and Use

- Some of the most effective current attacks on cyber networks worldwide exploit user behavior. These include phishing attacks, social engineering to obtain passwords, and introduction of malware via removable media.
- These threats are especially effective when directed at those with elevated network privileges and/or other elevated cyber responsibilities.
- Training users (privileged and unprivileged) and those with access to other pertinent information and media is a necessary deterrent to these methods. Organizations are expected to use risk-based analysis to determine the correct amount, content, and frequency of update to achieve minimal acceptable security in the area of influencing these behaviors, which affect cybersecurity.
- The metrics will be used to assess the extent to which organizations are providing adequate training to address these attacks and threats.[29]
- The introduction of the OPM EHRI data elements for cybersecurity personnel will aid in the identification of those professionals available to broaden the pool of skilled and educated workers capable of supporting a cyber-secure nation.[30]

8.1. Percent (%) of users that successfully completed[31] annual Cybersecurity Awareness and Training (CSAT). (KFM)

8.1.1. Percent (%) of new users who satisfactorily completed security awareness training before being granted network access or within an organizationally defined time limit that provides adequate security after being granted access. (KFM)

8.2. Percent (%) of all users that participated in cybersecurity-focused exercises. (KFM)

8.2.1. Percent (%) of the users in 8.2 that successfully completed exercises focusing on phishing, designed to increase awareness and/or measure effectiveness of previous training (e.g. organization conducts spoofed phishing emails, clicking link leads to phishing information page). (AP)

8.3. Percent (%) of the organization's network users and other staff[32] that have significant security responsibilities.[33] (KFM)

8.3.1. Percent (%) of the personnel counted in question 8.3 that have successfully completing role-based security training within the reporting year. (KFM)

---

[29] Even if the organization uses a DHS ISS-LOB, it remains the organization's responsibility to determine whether the content of the training is adequate to cover the threats it faces.

[30] The National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework is available at www.nist.gov/nice/framework.

[31] Successful completion means that the user has met the criteria of success as defined by the training service provider.

[32] "Other staff" means non-network users who may still have a significant impact on security. This group might include senior executives who do not use the network themselves but affect factors such as budget, staffing, and priorities. The size of this group is expected to be small.

[33] 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.

9. INCIDENT RESPONSE

Purpose and Use:

- Given real-world reports, it is reasonable to expect that some attacks will succeed. Organizations need to be able to detect those attacks. Ideally, organizations would defend against those attacks in real time, but at a minimum we expect organizations to determine the kinds of attacks that have been successful.
- Organizations can use this information about successful attacks and their impact to make informed risk-based decisions about where it is most cost effective and essential to focus security resources.
- In alignment with NIST 800-61 Rev 2, US-CERT has rolled out new incident reporting standards which take effect October 1, 2015, and can be found here.

9.1. Of the information security incidents reported to US-CERT in FY2015, what was the total number of incidents reported to Congress? (Base)

9.2. Of all of the cyber related (electronic) incidents with confirmed loss of confidentiality, integrity or availability reported to US-CERT in FY15 (per OMB M-15-01), what was the average meantime (in hours) between detection and notification to the Agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or Information Technology (IT) department? (Base)

9.3. When will the agency transition to the new US-CERT reporting format? (Base)

APPENDIX A: ANNUAL CIO METRIC ADDITIONAL METRIC CONTEXT

FY15 Annual FISMA CIO Metrics	Metric	Context
2.1	What is the total number of the organization's hardware assets connected to the organization's unclassified network(s)? (Base)	N/A
2.1.2	What is the total number of endpoints connected to the organization's unclassified network(s)? (Base)	N/A
2.2	Percent (%) of the organization's network fabric covered by a capability to detect and alert on the addition of unauthorized hardware assets onto the organization's network. (AP)	As it relates to FISMA, network fabric is defined as the overall total of the D/A's networked hardware assets. This includes the network topology of the organization, such as servers, storage, client machines, and other networked assets in a cohesive switched infrastructure. This may also be referred to as the Agency's network infrastructure(s). Portions of the network fabric that implement compensating controls such as disabling unused ports should be counted as meeting the intent of this metric.
2.3	Percent (%) of the organization's network fabric covered by an automatic capability (scans/device discovery processes) that provides enterprise-level visibility into the current state of all hardware assets. (AP)	As it relates to FISMA, network fabric is defined as the overall total of the D/A's networked hardware assets. This includes the network topology of the organization, such as servers, storage, client machines, and other networked assets in a cohesive switched infrastructure. This may also be referred to as the Agency's network infrastructure(s).
2.4	What is the mean time to detect a new device (time between scans in 2.2)? (AP)	N/A
2.6	Percent (%) of endpoints from 2.1.2 covered by an automated software asset inventory capability to scan the current state of installed software (e.g., .bat, .exe, .dll). (AP)	N/A
2.7	Percent (%) of endpoints from 2.1.2 covered by a desired-state software asset management capability to detect and block unauthorized software from executing (e.g., AppLocker, certificate, path, hash value, services, and behavior based whitelisting solutions). (AP)	N/A

FY15 Annual FISMA CIO Metrics	Metric	Context
2.10	Please complete Table 2. Future configurations will be added as needed. Data calls for layer 2, layer 3, mobile, printers, or other devices or operating systems will be used as needed.	N/A
2.11	Percent (%) of hardware assets listed in 2.1 assessed using credentialed scans with Security Content Automation Protocol (SCAP) validated vulnerability tools. (AP)	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 undergo any vulnerability scan with Security Content Automation Protocol (SCAP) validated vulnerability tools.
2.12	What is the mean time between vulnerability scans? (AP)	Based on credentialed scans in 2.11
2.14	What is the mean time to mitigate for high findings? (AP)	Based on credentialed scans in 2.11
3.1	How many users have unprivileged network accounts (Exclude privileged user accounts and non-user accounts)? (Base)	Total (3.1) = (number of users technologically required to log onto the network with a two-factor PIV card) + (number of users with PIV cards, but not required to use it) + (number of users without PIV cards).
3.1.1	Percent (%) of users from 3.1 technically required to log onto the network with a two-factor PIV card or NIST Level of Assurance (LOA) 4 credential. (AP)	100% (3.1.1) = Percent (%) of users from 3.1 technologically required to log onto the network with a two-factor PIV card. Please note the context information for 3.1. A policy document requiring PIV use is not sufficient.
3.2	How many users have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.) (KFM)	Total (3.2) = (number of users technologically required to log onto the network with a two-factor PIV card) + (number of users with PIV cards, but not required to use it) + (number of users without PIV cards).
3.2.1	Percent (%) of users from 2.2 technically required to log onto the network with a two-factor PIV card or NIST Level of Assurance (LOA) 4 credential. (AP)	100% (3.2.1) = Percent (%) of users from 3.2 technologically required to log onto the network with a two-factor PIV card. Please note the context information for 3.2. A policy document requiring PIV use is not sufficient.
4.1	Percent (%) of privileged user accounts that have a technical control preventing internet access. (AP)	Based on user accounts from 3.2
4.2	Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.

FY15 Annual FISMA CIO Metrics	Metric	Context
4.3	Percent (%) of hardware assets covered by a host-based intrusion prevention system. (AP)	Based on assets in 2.1
4.4	Percent (%) of hardware assets covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information. (AP)	Based on assets in 2.1.2 Percent (%) of hardware assets covered by an antivirus (AV) or "intrusion prevention solution" using file reputation services, checking files against cloud-hosted, continuously updated malware information.
4.5	Percent (%) of email attachments opened in sandboxed environment or detonation chamber. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
4.6	Percent (%) of incoming emails using email sender authentication protocols such as DomainKeys Identified Mail (DKIM), Author Domain Signing Practices (ADSP), Domain-based Message Authentication, Reporting & Conformance (DMARC), Vouch by Reference (VBR), or IP Reverse (iprev). (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
4.7	Percent (%) of incoming emails scanned using a reputation filter tool to perform threat assessment of email sender. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
4.8	Percent (%) of hardware assets covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar). (AP)	Based on assets in 2.1
4.9	Percent (%) of inbound email traffic passing through anti-phishing/anti-spam filtration technology at the outermost border Mail Transport Agent or email server. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
4.10	Percent (%) of inbound network traffic that passes through a web content filter that provides anti-phishing, anti-malware, and blocking of malicious websites (e.g. fake software updates, fake antivirus offers, and phishing offers). (AP)	N/A
4.11	Percent (%) of hardware assets that have implemented a browser-based (e.g. Microsoft Phishing filter) or enterprise-based tool to block known phishing websites and IP addresses. (AP)	Based on assets in 2.1.2

FY15 Annual FISMA CIO Metrics	Metric	Context
4.12	Percent (%) of outbound communications traffic checked at the external boundaries to detect covert exfiltration of information. (AP)	N/A
4.13	Percent (%) of sent email that is digitally signed. (AP)	This is not to collect the percent of email messages digitally signed by individuals' certs; rather, it is the outbound equivalent to "4.6. Incoming emails using email sender authentication protocols such as DomainKeys Identified Mail (DKIM), Author Domain Signing Practices (ADSP), Domain-based Message Authentication, Reporting & Conformance (DMARC), Vouch by Reference (VBR), or IP Reverse (iprev)". This metric is to track the percent of email processed by email systems with this functionality implemented and in use.
4.14	Percent (%) of email traffic quarantined or otherwise blocked. (AP)	Percent of email traffic processed by email systems with this functionality implemented and in use.
6.1.4	Percent (%) of remote access connections scanned for malware upon connection. (AP)	Remote access connections are defined as the ability for an organization's users to access its non-public computing resources from locations external to the organization's facilities. This applies to remote access solutions that protect access to the organization's desktop LAN/WAN resources and services. Remote access excludes non-GFE systems using externally facing applications (e.g., Outlook Web Access, Remote Desktop/Citrix Solutions, Good Messaging, etc.).
8.2.1	Percent (%) of the users that participated in cybersecurity-focused exercises who successfully completed exercises focusing on phishing, designed to increase awareness and/or measure effectiveness of previous training (e.g., organization conducts spoofed phishing emails, clicking link leads to phishing information page). (AP)	N/A

Table 4: FY15 FISMA Metrics and Context

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 %**	**FY15 Annual FISMA CIO Metrics**	**Agency Calculation**
Information Security Continuous Monitoring (ISCM)			
Hardware Asset Management	≥ 95%	2.2, 2.3	Both results must be greater than or equal to target
Software Asset Management	≥ 95%	2.6, 2.7	Both results must be greater than or equal to target
Vulnerability and Weakness Management	≥ 95%	2.11	Result must be greater than or equal to target
Secure Configuration Management	≥ 95%	2.10.6	Result must be greater than or equal to target
Identity and Credential Access Management (ICAM)			
Unprivileged Network Users	≥ 85%	3.1.1	Result must be greater than or equal to target
Privileged Network Users	100%	3.2.1	Result must equal target
Anti-Phishing and Malware Defense			
Anti-Phishing Defense	≥ 90%	4.2, 4.5, 4.6, 4.7, 4.9, 4.13, 8.2.1	Top 5 results must be greater than or equal to target
Malware Defense	≥ 90%	4.3, 4.4, 4.8, 4.11, 6.1.4	Top 3 results must be greater than or equal to target
Blended Defense	≥ 90%	4.1, 4.10, 4.12, 4.14	Top 2 results must be greater than or equal to target

Table 5: Summary of CAP Goal Target & Methodology

APPENDIX C: DEFINITIONS

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.

Current (Actual) State

Set of all devices actually on the network at any moment. The actual state includes all authorized, unauthorized, managed, and unmanaged devices on the network. The actual state inventory is the best available list of the current actual state devices.

Desired State

The Hardware Asset Management desired state is a list of the hardware assets (devices) expected to be on the network. The list of desired state hardware assets should:

- be created through a repeatable process
- include only authorized devices
- assign each authorized device for technical management of settings, software, patching, etc.

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.

Hardware assets

Organizations have tended to divide these assets into the following categories for internal reporting. (Note: Those that do not meet the criteria defined below should be excluded.) The detailed lists under each broad category are illustrative and not exhaustive. Note that the last category, "other addressable devices on the network," addresses the criterion for including other kinds of specialized devices not explicitly called out.

- endpoints[34]
  - servers
  - workstations (desktops)
  - laptops
  - net-books
- mobile devices
  - Blackberry
  - iPhone
  - Android
  - Tablets

[34] 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.

- networking devices[35]
  - 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
  - modems
- other communication devices
  - encryptors
  - decryptors
  - VPN
  - alarms and physical access control devices
  - PKI infrastructure[36]
- Other input/output devices if they appear with their own address
  - network printers/plotters/copiers/multi-function devices (IP addressable)
  - network fax portals
  - network scanners
  - network accessible storage devices
  - VOIP phones
  - others network input/output devices
- Virtual machines that can be addressed[37] as if they are a separate physical machine should be counted as separate assets,[38] including dynamic and on-demand virtual environments.
- other devices addressable on the network

Both Government Furnished Equipment (GFE) assets and non-GFE assets are included if they meet the other criteria for inclusion listed here.[39] 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.

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

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

[37] "Addressable" means by IP address or any other method to communicate to the network.

[38] 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://www.gsa.gov/portal/category/102371.

[39] 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.

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

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

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. wirelessly transmit or receive 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 Fabric

As it relates to FISMA, this is defined as the overall total of the Agency's networked hardware assets. This includes the network topology of the organization, such as servers, storage, client machines, and other networked assets in a cohesive switched infrastructure. This may also be referred to as the Agency's network infrastructure(s).

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[40] or (b) created to establish a service (like a group mailbox), and no one is expected to log into the account.

PIV credentials

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)

Privileged network account

A network account with elevated privileges which is typically allocated to system administrators, network administrators, DBAs, 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.

[40] For example, this includes machine accounts and operating system built-in accounts. More generally, it includes "service" accounts.

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

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

S/MIME (secure/multipurpose internet mail extensions)
A set of specifications for securing electronic mail. Secure/ Multipurpose Internet Mail Extensions (S/MIME) is based upon the widely used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s).

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 on OMB's MAX Portal.

TIC/MTIPS (trusted internet connections/managed trusted internet protocol services)
A GSA program described by both DHS and GSA.

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

APPENDIX D: ACRONYMS

ADSP	Author Domain Signing Practices
AO	Authorizing Official
AP	Administration Priorities
ATO	Authority to Operate
AV	Antivirus
BASE	Baseline Questions
CA	Certificate Authority and/or Certification Authority
CAP	Cross Agency Priority
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CM	Continuous Monitoring
ConOps	Concept of Operations
CPU	Central Processing Unit
CSAT	Cybersecurity Awareness and Training
D/A	Department/Agency
DBA	Database Administrator
DHS	Department of Homeland Security
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting & Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
EMET	Enhanced Mitigation Experience Toolkit
FAQ	Frequently Asked Questions
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity Credential and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FNR	Federal Network Resilience
FY	Fiscal Year

GFE	Government Furnished Equipment
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
IP	Internet Protocol
ICAM	Identity Credential and Access Management
ISCM	Information Security Continuous Monitoring
ISP	Internet Service Provider
ISS-LOB	Information Systems Security Line of Business
JCMWG	Joint Continuous Monitoring Working Group
KFM	Key FISMA Metrics
LAN	Local Area Network
LOA	Level of Assurance
MTIPS	Managed Trusted Internet Protocol Services
NAT	Network Address Translators
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NSA	National Security Agency
OMB	Office of Management and Budget
OPM EHRI	Office of Personnel Management Enterprise Human Resources Integration
OS	Operating System
PACS	Physical Access Control Systems
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
RA	Registration Authority
RMF	Risk Management Framework
S/MIME	Secure/Multipurpose Internet Mail Extensions
SBU	Sensitive but Unclassified
SCAP	Secure Content Automation Program
TIC	Trust Internet Connections
URL	Uniform Resource Locator

US-CERT	United States Computer Emergency Readiness Team
VBR	Vouch by Reference
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX E: REQUIREMENTS AND BEST PRACTICES IMPLEMENTATION GUIDANCE

FY15 Metric	Source
1.1. For each FIPS 199 impact level, what is the total 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.	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • FISMA: Section 3505(c)(1) • FIPS-199: Section 2 & 1 • FIPS-200: Paragraph 3, page iv and paragraph 11, page v; Section 1, 2 & 4 • NIST SP 800-60: Section 1.1; Section 2.5; Section 3.0; Section 4.0, Step 2, page 13; Section 4.1, Step 1 • NIST 800-53 Rev4: page x; Sections 1.1, 1.4, 2.1 & 4.1; RA-2
1.1.1. Organization-Operated Systems	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • FISMA: Section 3505(c)(1) • FIPS-199: Section 2 & 1 • FIPS-200: Paragraph 3, page iv and paragraph 11, page v; Section 1, 2 & 4 • NIST SP 800-60: Section 1.1; Section 2.5; Section 3.0; Section 4.0, Step 2, page 13; Section 4.1, Step 1 • NIST 800-53 Rev4: page x; Sections 1.1, 1.4, 2.1 & 4.1; RA-2
1.1.2. Contractor-Operated Systems	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • FISMA: Section 3505(c)(1) • FIPS-199: Section 2 & 1 • FIPS-200: Paragraph 3, page iv and paragraph 11, page v; Section 1, 2 & 4 • NIST SP 800-60: Section 1.1; Section 2.5; Section 3.0; Section 4.0, Step 2, page 13; Section 4.1, Step 1 • NIST 800-53 Rev4: page x; Sections 1.1, 1.4, 2.1 & 4.1; RA-2

FY15 Metric	Source
1.1.3. Systems (from 1.1.1 and 1.1.2) with Security ATO (signed, in-scope)	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • FISMA: Section 3505(c)(1) • FIPS-199: Section 2 & 1 • FIPS-200: Paragraph 3, page iv and paragraph 11, page v; Section 1, 2 & 4 • NIST SP 800-60: Section 1.1; Section 2.5; Section 3.0; Section 4.0, Step 2, page 13; Section 4.1, Step 1 • NIST SP 800-37 Rev1: page iii; Section 3.1 • NIST 800-53 Rev4: page x "Authority"; Sections 1.1, 1.4, 2.1 & 4.1; RA-2
1.2. How many endpoints belong to systems without a valid ATO?	• FIPS-200: Section 3 • NIST SP 800-37 Rev1: page iii; Appendix F; • NIST SP 800-53, r4 CA-6
1.3 How many public facing systems are without a valid ATO?	• FIPS-200: Section 3 • NIST SP 800-37 Rev1: page iii; Appendix F; • NIST SP 800-53, r4 CA-6
2.1. What is the total number of the organization's hardware assets connected to the organization's unclassified network(s)?	• M-10-15 pg. 1-2 • FIPS-200 Section 3
2.1.1. Percent (%) of assets from 2.1 that store (e.g., on an endpoint or maintained as a record in an external asset management database) meta-data (e.g. system association, owner, location)?	• NIST SP 800-53 Rev4: AC-4(6)
2.1.2. What is the total number of endpoints connected to the organization's unclassified network(s)?	• NIST SP 800-53 Rev4: CA-7 (a), (d), M-10-15: page 1-2
2.2. Percent (%) of the organization's network fabric covered by a capability to detect and alert on the addition of unauthorized hardware assets onto the organization's network.	• NIST SP 800-53 Rev4: CM-8(3); Appendix B (Mandatory Access Control)
2.3. Percent (%) of the organization's network fabric covered by an automatic capability (scans/device discovery processes) that provides enterprise-level visibility into the current state of all hardware assets.	• M-10-15: page 1-2, #11 • M-14-03: page 1, 7, 10 • NIST SP 800-53 Rev4: CM-8, (2), (5); CA-7 • NIST SP800-137: page 1;
2.4 What is the mean time to detect a new device (time between scans in 2.2)?	• NIST SP 800-53 Rev4: CM-8(3)(a)

FY15 Metric	Source
2.5. Percent (%) of the organization's registered network fabric covered by a Network Access Control switching technology that blocks unauthorized devices.	• NIST SP 800-115
2.6. Percent (%) of endpoints from 2.1.2 covered by an automated software asset inventory capability to scan the current state of installed software (e.g., .bat, .exe, .dll).	• NIST SP 800-53, r4 CM-2, CM- 6, CM-8(6) • NIST SP 800-128
2.7. Percent (%) of endpoints from 2.1.2 covered by a desired-state software asset management capability to detect and block unauthorized software from executing (e.g. AppLocker, certificate, path, hash value, services, and behavior based whitelisting solutions).	• NIST SP 800-53, r4 CA-7, CM-7(5), RA-5 • NIST SP 800-128
2.8. How many major application databases does the organization maintain?	• NIST SP 800-123
2.9. Percent (%) of the organization's network fabric that undergoes periodic discovery scanning specifically for the purpose of identifying and enumerating databases.	• NIST SP 800-123
2.10.1. What is the number of hardware assets with each OS?	• NIST SP 800-53, r4, CA-7
2.10.2. What is the common security configuration baseline for each OS listed (e.g. USGCB)?	• NIST SP 800-53, r4,CM-2, CM- 6 • NIST SP 800-128
2.10.3. How many configuration exceptions are granted by the enterprise?	• NIST SP 800-53, r4,CM-2, CM- 6 • NIST SP 800-128
2.10.4. What is organization's enterprise policy for maximum audit interval (target)?	• NIST SP 800-123, Section 3.3 • SP 800-53, Rev4 (AU-2 (d), AU-6 (c))
2.10.5. What is organization's enterprise average audit interval (actual)?	• NIST SP 800-123, Section 3.3
2.10.6. Percent (%) of assets in 2.10.1 covered by the auditing activities described in 2.10.3 and 2.10.4.	• NIST SP 800-123, Section 3.3
2.11. Percent (%) of hardware assets listed in 2.1 assessed using credentialed scans with Security Content Automation Protocol (SCAP) validated vulnerability tools.	• NIST SP 800-53, r4 CA-7, CM-6 • NIST SP 800-128
2.12. What is the mean time between vulnerability scans?	•
2.13. Percent (%) of the databases in 2.8 that undergo periodic vulnerability scanning with a special purpose database vulnerability scanner.	• NIST SP 800-128, Section 2.3.6
2.14. What is the mean time to mitigate for high findings?	• NIST SP 800-128, Section 2.3.6

FY15 Metric	Source
3.1. How many users have unprivileged network accounts? (Exclude privileged network accounts and non-user accounts.)	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • HSPD-12 • OMB M-14-04 • FIPS-199 • FIPS-200 • FIPS-201-2 • NIST SP 800-53 r4, IA-2(2)
3.1.1. Percent (%) of users from 3.1 technically required to log onto the network with a two-factor PIV card.	• FICAM Roadmap and Implementation Guidance, V2.0 Chapter 9, 11 • OMB M-11-11 • NIST SP 800-53 r4, IA-2 (2)
3.2. How many users have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • HSPD-12 • OMB M-04-04 • FIPS-199 • FIPS-200 • FIPS-201 • NIST SP 800-53 r4 IA-2 (1)
3.2.1. Percent (%) of users from 3.2 technically required to log onto the network with a two-factor PIV card.	• FICAM Roadmap and Implementation Guidance, V2.0, Chapter 9, 11 • OMB M-11-11 • NIST SP 800-53 r4 IA-2 (1)
3.3. Percent (%) of privileged network users that had their privileges reviewed this year.	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • HSPD-12 • OMB M-04-04 • FIPS-199 • FIPS-200 • FIPS-201-2 • NIST 800-53, r4 AC-6
3.4. Percent (%) of privileged network users that had their privileges adjusted or terminated after being reviewed this year.	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • HSPD-12 • OMB M-14-04 • FIPS-199 • FIPS-200 • FIPS-201-2 • NIST 800-53, r4 AC-2(7)

FY15 Metric	Source
3.5. Percent (%) of the organization's internal systems configured to require PIV authentication.	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • HSPD-12 • OMB M-04-04 • FIPS-199 • FIPS-200 • FIPS-201-2 • NIST 800-53, r4 IA-2
3.6. Percent (%) of the organization's government service portals (e.g., Max.gov Portal, MyEPP) that enforce PIV authentication for cross-agency federal customers (if none are provided, answer N/A).	• FICAM Roadmap and Implementation Guidance, v2, Chapter 8, 10, 12 • OMB M-11-11 • NIST SP 800-53, r4 IA-8(1)
3.7. How many users log onto the organization's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services?	• NIST SP 800-53, r4 IA-2, AC- 17 • NIST 800-63
3.7.1. Percent (%) of the users reported in 3.7 required to use two-factor PIV card authentication to remotely log onto the organization's desktop LAN/WAN resources or services.	• FICAM Roadmap and Implementation Guidance, V2.0 Chapter 9, 11 • OMB M-11-11 • NIST SP 800-53, r4 IA-2, AC- 17
3.8 How many users are enabled to remotely log onto the organization's LAN/WAN resources or services from mobile devices?	• FICAM Roadmap and Implementation Guidance, V2.0 Chapter 9, 11 • OMB M-11-11
3.8.1. Of the organization's users who remotely access desktop LAN/WAN resources or services from mobile devices, what percent (%) of these users are technically required to use two-factor PIV card authentication to access these resources and services?	• FICAM Roadmap and Implementation Guidance, V2.0 Chapter 9, 11 • OMB M-11-11
3.9. Percent (%) of agency's operational Physical Access Control Systems (PACS) that comply with procurement requirements for purchasing products and services from the FIPS 201 Approval Products List maintained by General Services Administration (GSA) (per OMB M-06-18).	• OMB M-06-18 • NIST SP 800-116, Section 6.4, 8.7
3.10. 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 201-1 and NIST SP 800-116).	• NIST SP 800-116 • FIPS 201-1
4.1. Percent (%) of privileged user accounts have a technical control preventing internet access.	• NIST 800-53, R4 - AC-6 (2)
4.2. Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments.	• NIST SP 800-53, r4 AC-4 (1), SI-3 • NIST SP 800-45, r2 Chapter 6

FY15 Metric	Source
4.3. Percent (%) of hardware assets covered by a host-based intrusion prevention system.	• NIST SP 800-53 r4, SI-4(1)
4.4. Percent (%) of hardware assets covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information.	• NSA Slick Sheet: Anti-Virus File Reputation Services • NIST SP 800-53, r4 SI-3(2)
4.5. Percent (%) of email attachments opened in sandboxed environment or detonation chamber.	• NIST SP 800-53, r4 SC-44
4.6. Percent (%) of incoming emails using DomainKeys Identified Mail (DKIM) or other email authentication, such as ADSP, DMARC, VBR, or iprev.	• NIST SP 800-53, r4 SC-20
4.7. Percent (%) of incoming emails scanned using a reputation filter tool to perform threat assessment of email sender.	• NIST SP 800-45, r2 Chapter 6
4.8. Percent (%) of hardware assets covered by an anti-exploitation tool (e.g., EMET or similar).	• NSA Slick Sheet: Anti-Exploitation Features • NIST SP 800-53, r4 SI-3(7)
4.9. Percent (%) of inbound network traffic passes through anti-phishing/anti-spam filtration technology at the outermost border Mail Transport Agent or email server.	• NIST SP 800-53, r4 SI-8 • NIST SP 800-45
4.10. Percent (%) of inbound network traffic that passes through a web content filter that provides anti-phishing, anti-malware, and blocking of malicious websites (e.g. fake software updates, fake antivirus offers, and phishing offers).	• NIST SP 800-53, r4 SI-3, SI- 7(8)
4.11. Percent (%) of hardware assets that have implemented a browser-based (e.g. Microsoft Phishing filter) or enterprise-based tool to block known phishing websites and IP addresses.	• NIST SP 800-45
4.12. Percent (%) of outbound communications traffic checked at the external boundaries to detect covert exfiltration of information.	• NIST SP 800-53, r4 SI-4 (4)(18), SC-7 (10)
4.13. Percent (%) of sent email is digitally signed.	• NIST SP 800-45, r2 Chapter 3
4.14. Percent (%) of email traffic quarantined or otherwise blocked.	•
5.1. What is the estimated number of hardware assets in each of the following mobile and portable asset types, and how many are encrypted?	• FISMA: Section 3544(a)(1)(A) • FISMA: Section 3554(a)(1)(A) • FIPS-199 • FIPS-200 • NIST SP 800-53, r4 AC-19(5)
6.1. What is the estimated percent (%) of remote access connections that have each of the following properties:	See 6.1.1.-6.1.4. for sources
6.1.1. Percent (%) that utilize FIPS 140-2-validated cryptographic modules.	• NIST SP 800-53, r4 AC-17(2)
6.1.2. Percent (%) that prohibit split tunneling and/or dual-connected remote hosts where the mobile device has two active connections.	• NIST 800-53, r4 SC-7(7)

FY15 Metric	Source
6.1.3. Percent (%) configured in accordance with OMB M-07-16 to time-out after 30 minutes of inactivity (or less) and requires re-authentication to reestablish session.	• OMB M-07-16 • NIST SP 800-53, r4 SC-10
6.1.4. Percent (%) scanned for malware upon connection.	• NIST SP 800-46, r1 Chapter 3 • NIST SP 800-83
7.1. Percent (%) of the required TIC 2.0 Capabilities implemented.	• FISMA: Section 3545 • CNCI Initiative #1 • OMB M-08-05 • OMB M-08-16 • OMB M-08-27 • Cyberspace Policy Review (pg. 24, 2009)
7.2. Percent (%) of external network traffic to/from the organization's networks that passes through a TIC/MTIPS.	• FISMA: Section 3544 b-1-a, b • FISMA: Section 3554(b) • FISMA Section 3545 • OMB M-08-05 • OMB M-08-27 • Cyberspace Policy Review (pg.24, 2009)
7.3. Percent (%) of external network/application interconnections to/from the organization's networks that passes through a TIC/MTIPS.	• FISMA: Section 3544 b-1-a, b • FISMA: Section 3554(b) • FISMA Section 3545 • CNCI Initiative #1 • NIST SP 800-53, r4 SC-7(1)
7.4. Percent (%) of public-facing servers use IPv6 (e.g., web servers, email servers, DNS servers, etc.). (Exclude low-impact networks, cloud servers, and Internet Service Provider (ISP) resources unless they require IPv6 to perform their business function.)	• NIST SP 800-119
8.1. Percent (%) of users that successfully completed annual Cybersecurity Awareness and Training (CSAT).	• FISMA: Section 3544(b)(4) • FISMA: Section 3554(b)(4) • A-130 Section 9(f)(a) • OMB M-07-16 Section 2(d) • NIST SP 800-53 r4 AT-2 • NIST SP 800-16 Revision 1
8.1.1. Percent (%) of new users who satisfactorily completed security awareness training before being granted network access or within an organizationally defined time limit that provides adequate security after being granted access.	• FISMA: Section 3544(b)(4) • FISMA: Section 3554(b)(4) • A-130 Section 9(f)(a) • OMB M-07-16 Section 2(d) • NIST SP 800-53 r4 AT-2
8.2. Percent (%) of all users that participated in cybersecurity-focused exercises.	• NIST SP 800-84 • NIST SP 800-53, r4 AT-2(1)

FY15 Metric	
8.2.1. Percent (%) of the users in 8.2 that successfully completed exercises focusing on phishing, designed to increase awareness and/or measure effectiveness of previous training. (e.g., organization conducts spoofed phishing emails, clicking link leads to phishing information page)	• NIST SP 800-53 r4 AT-2
8.3. Percent (%) of the organization's network users and other staff that have significant security responsibilities.	• FISMA: Section 3544(a)(3)(D) • FISMA: Section 3554(a)(3)(D) • NIST SP 800-53, r4 AT-3
8.3.1. Percent (%) of the personnel counted in question 8.1 successfully completed role-based security training within the past year.	• FISMA: Section 3544(a)(3)(D) • FISMA: Section 3554(a)(3)(D) • NIST SP 800-53 r4 AT-3
9.1. Of the information security incidents reported to US-CERT in FY2015, what was the total number of incidents reported to Congress?	• US-CERT Federal Incident Notification Guidelines
9.2. Of all of the cyber related (electronic) incidents with confirmed loss of confidentiality, integrity or availability reported to US-CERT in FY15 (per OMB M-15-01), what was the average meantime (in hours) between detection and notification to the Agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or Information Technology (IT) department?	• US-CERT Federal Incident Notification Guidelines
9.3. When will the agency transition to the new US-CERT reporting format?	• US-CERT Federal Incident Notification Guidelines