Homeland Security

DHS 4300A
Sensitive Systems Handbook

Attachment E

FISMA Reporting

Version 11.0
August 5, 2014

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
1.0	September 9, 2004	Initial release
2.0	July 29, 2005	Minor editorial changes
2.1	October 1, 2005	Clarification of policy c in Section 5.0.
2.2	December 30, 2005	Modification to policy c in Section 5.0; addition of policies d & e.
4.0	June 1, 2006	Change to policy c in Section 5.0, minor editorial changes.
5.0	March 1, 2007	No change
6.0	May 14, 2008	No change.
6.1	September 23, 2008	Included “Interconnnection Security Agreements Template” as an appendix.
7.0	August 7, 2009	Introduced new terminology Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53
8.0	July 19, 2011	Updated NIST 800-37 terminology Aligned Appendix N4 with RMS template
11.0	August 5, 2014	Changes to: References, Figure 1, IACS, FNR, and the annual FISMA questions References updated. References to DoD reporting removed. Stylistic editing.

Contents

1.0 INTRODUCTION 1
1.1 Purpose 1
1.2 Background 1
1.3 Scope 2
1.4 References 2
2.0 OMB REPORTING REQUIREMENTS 3
2.1 Secretary's Annual FISMA Report 3
2.2 CIO Quarterly FISMA Report 4
3.0 DHS SECURITY MANAGEMENT TOOLS 5
3.1 Enterprise FISMA Compliance and Security Authorization Tool 6
3.2 Management Aggregation and Security Tool (MAST) 7
3.3 ISO Reporting Tool 8
3.4 Accessing DHS Security Management Tools 8
3.5 Customer Service Center 8
4.0 COMPONENT FISMA REPORTING 9
4.1 Annual FISMA Data Requirements 9
4.2 Quarterly Reporting Requirements 15
5.0 RESPONSIBILITIES 17
5.1 Chief Information Officer 17
5.2 Chief Information Security Officer 17
5.3 Component Chief Information Officer 17
5.4 System Owners and Program Officials 17
5.5 Component Chief Information Security Officers and Information System Security Managers 18
5.6 Information system Security Officers 18
6.0 DEPARTMENT SCORECARD 19

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to provide information as to how Department of Homeland Security (DHS) Components and reporting offices assist the Chief Information Officer (CIO) in following the Office of Management and Budget's (OMB) annual reporting guidance for the Federal Information Security Management Act (FISMA). This document also provides metrics defined by DHS Federal Network Resiliency (FNR).

This document provides guidance for handling every category of information systems security metrics and applies to DHS Headquarters, to all DHS Components, to DHS Data Centers, and to any company, consultant, partner, or Government agency that is receiving Federal funds from DHS or performing a Federal function on behalf of or in cooperation with DHS.

1.2 Background

FISMA was created to achieve the following objectives:

- Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.
- Recognize the highly networked nature of the current Federal computing environment and provide effective Government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities.
- Provide for development and maintenance of minimum controls required to protect Federal information and information systems.
- Provide a mechanism for improved oversight of Federal agency information security programs.
- Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector
- Recognize that the selection from among commercially developed products of specific technical hardware and software information security solutions should be left to individual agencies.

FISMA requires OMB to oversee agencies' progress in implementing the Act's requirements. Following OMB guidance, DHS submits monthly, quarterly and annual FISMA reports to OMB on the status, adequacy, and effectiveness of the Department's information security policies, procedures, and practices, and on the status of compliance with FISMA requirements. Much of the required data shows the degree of each Component's compliance with IT system metrics established by FISMA. The DHS FISMA reporting process relies on timely entry of data by system owners and information security professionals into DHS security management tools and on submittal of monthly scanning tool data feeds.

In July of 2010, OMB named DHS Federal Network Resiliency (FNR) Branch as the agency that will exercise primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect FISMA. FNR requires monthly, quarterly, and annual reporting of key metrics through the Cyberscope tool.

1.3 Scope

Components will use the DHS Information Assurance Compliance System (IACS) to develop, maintain, and monitor Security Authorization Packages (SAP) for all Sensitive But Unclassified (SBU) IT Systems. A separate instance of CIACS (Classified IACS) is used as the repository for systems at the SECRET level and at the TOP SECRET level. Those systems classified as Sensitive Compartmentalized Information (SCI) fall under the responsibility of the Office of Intelligence and Analysis for FISMA reporting purposes.

1.4 References

Federal Laws

Federal Information Security Management Act of 2002, 44 USC 3541 et seq., enacted as Title III of the E-Government Act of 2002, Pub L 107-347, 116 Stat 2899

Office of Management and Budget (OMB) Memorandums

OMB Memorandum M-10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS), M-10-28, July 6, 2010.

OMB Memorandum M-12-20, "FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, Office of Management and Budget, M-12-20, September 27, 2012 (or successor).

National Institute of Standards and Technology (NIST) Special Publications (SP)

NIST SP 800-53, Rev 4, "Recommended Security Controls for Federal Information Systems and Organizations," (April 30, 2013)

Department of Homeland Security Publications

"DHS Information Security Program Plan of Action and Milestones (POA&M) Process Guide," Attachment H to DHS 4300A Sensitive Systems Handbook, June 2012

"FY 2013 Chief Information Officer Federal Information Security Management Act Reporting Metrics," DHS National Cyber Security Division, Federal Network Resilience. November 2012.

2.0 OMB REPORTING REQUIREMENTS

OMB requires all Federal agencies to provide monthly, quarterly, and annual FISMA reports as follows:

Month	Report
January	Quarterly Report to OMB
April	Quarterly Reports to OMB
July	Quarterly Report to OMB
November	Annual FISMA Report to OMB

Table 1: Schedule of FISMA Reports

2.1 Secretary's Annual FISMA Report

Each November, the Secretary of Homeland Security is required to provide the FNR via the OMB Cyberscope application, a report that summarizes Department's progress in meeting FISMA requirements. The report includes the results of annual IT security reviews of systems. Under FISMA, DHS must report on all agency systems including national security systems**.** The DHS CIO metrics are derived from 3 different sources:

- Administration Priorities
- Key FISMA Metrics
- Baseline Questions

Throughout the year this data is obtained using current approved compliance tools, scan data from tools such as Nessus, McAfee, and BigFix as well as component data calls. The responses are aggregated for all systems by Component and then entered into the Cyberscope application.

In FY11 the Administration identified three FISMA priorities:

1. Continuous Monitoring
2. Trusted Internet Connection (TIC) capabilities and traffic consolidation
3. Implementation of Homeland Security Presidential Directive (HSPD)-12 for logical access control

In FY13, these priorities continue to provide emphasis on FISMA metrics that are identified as having the greatest probability of success in mitigating cybersecurity risks to agency information systems.

The Secretary's Annual Report, consists of the following:

- Transmittal letter from the Secretary, including a discussion of any differences between the findings of the agency CIO and the Inspector General (IG)
- Report on the CIO's annual IT security reviews of systems and programs
- Report on the IG independent evaluation of the DHS Information Security Program
- Status of agency compliance with OMB privacy policies completed by the Senior Agency Official for Privacy (SAOP)

After review by and notification from OMB, the Department forwards the transmittal letter with report to the appropriate Congressional Committees and to the General Accounting Office (GAO).

- For an interim approval, AOs specify tasks remaining to be completed and schedules for these tasks.
- For a rejected interconnection, return to the applicable planning steps.
- Perform a re-authorization through the security authorization process.

2.2 CIO Quarterly FISMA Report

The DHS CIO must provide an update on IT security performance measures to OMB per FISMA reporting requirements. These quarterly updates are due in January, April and July. A Quarterly report for 4th quarter is not required. Senior Agency Official for Privacy (SOAP) metrics are reported on the same schedule. OMB uses these quarterly reports to monitor the progress of DHS remediation efforts and to identify progress and problems.

3.0 DHS SECURITY MANAGEMENT TOOLS

In order to maintain consistent security processes and procedures across the Department, the DHS Chief Information Security Officer (CISO) has implemented the following web-based commercial off the shelf (COTS) security management tools:

- Information Assurance Compliance System (IACS)
- Management Aggregation and Security Tool (MAST)
- SAP 's Crystal Reports

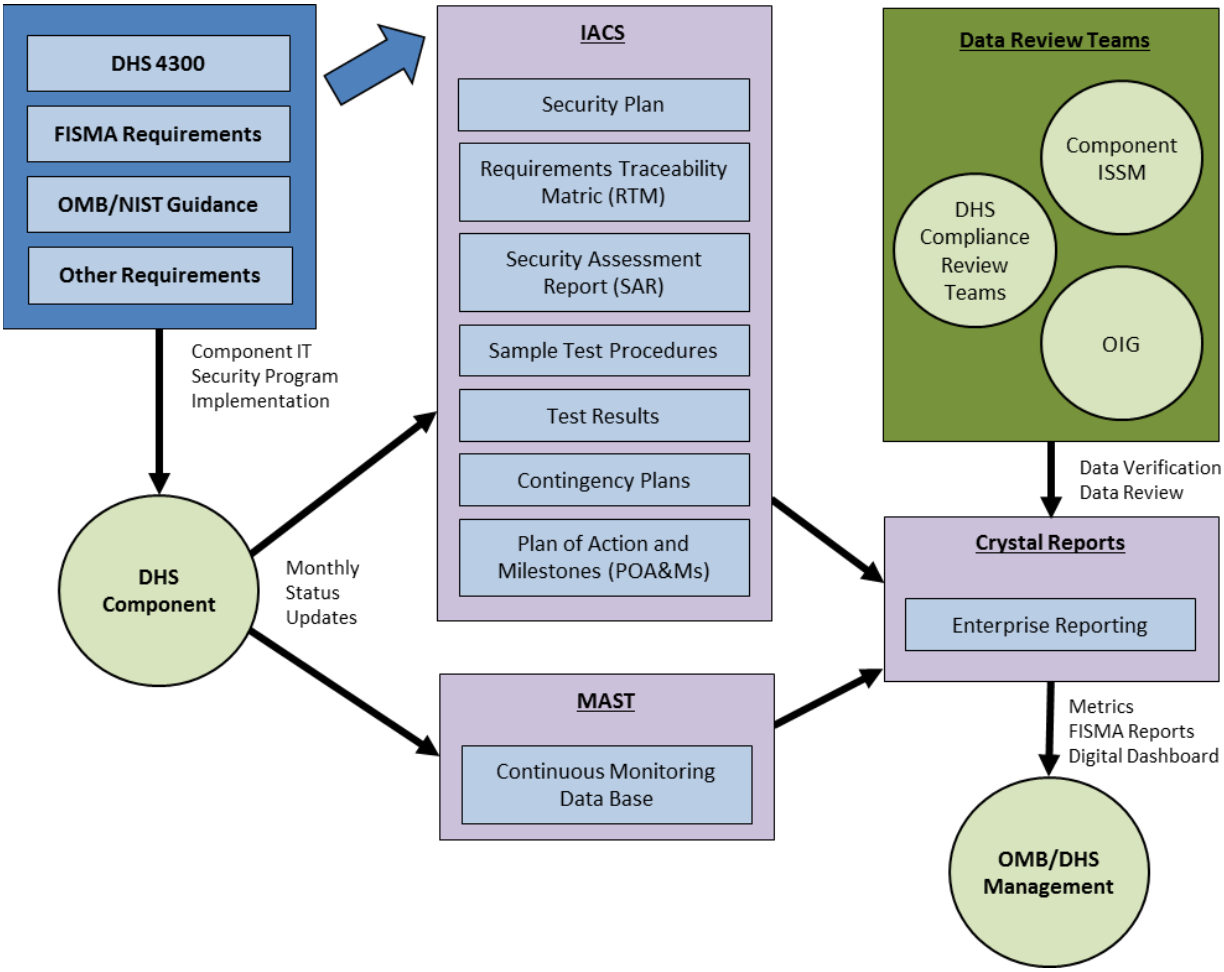

Figure 1: Enterprise security management tools that support FISMA

Figure 1 illustrates how the COTS enterprise security management tools are used by the Department to collect, manage, and report information security metrics. The diagram illustrates the following characteristics of the Department's FISMA reporting process:

- The security management tools incorporate DHS and federal information security mandates and foster Component compliance.
- Several types of data reviews are performed to verify the contents of the data in these tools and Component compliance:
  - The Component Chief Information Security Officer (CISO) or Information System Security Manager (ISSM) is responsible for verifying that the information is valid.

- In its annual independent review of the Department's information security program, the Office of the Inspector General (OIG) reviews a sample of the IT system data and assesses the quality of the data.
- The DHS CISO provides compliance review teams to assist the Components to improve their information security programs, processes, and procedures.

- OMB-mandated FISMA reports are automatically generated from the ISO Reporting tool.
- Information security metrics for each Component and for the Department are provided to senior DHS management through the monthly Information Security FISMA Scorecard.

3.1 Enterprise FISMA Compliance and Security Authorization Tool

The DHS FISMA Compliance tool, IACS, automates the collection and maintenance of FISMA data used for reporting to OMB. The tool provides a single, standard, consistent FISMA data collection and reporting process for ensuring that DHS is in compliance with OMB requirements. IACS automates and standardizes the labor-intensive data collection and reporting processes traditionally used to gather and report FISMA data.

IACS is also the Security Authorization (SA) tool for automating and standardizing portions of the SA process to assist DHS in quickly and efficiently developing security authorization packages. IACS utilizes questionnaires and templates to filter a master set of DHS security requirements so as to identify the subset of policies applicable to a specific IT system undergoing security authorization.

In support of FISMA and the Security Authorization Process, IACS provides the following functionality:

- Inventory Management
  - Stores information data for systems, sites, and programs
  - Aligns inventory data with the organizational structure of the Department
  - Provides an authoritative list of IT systems based on accreditation boundaries
  - Tracks key information points of contact for systems, sites, and programs
- Security Assessment and Performance
  - Allows National Institute of Standards and Technology (NIST) SP (Special Publication) 800-53, rev 4 security controls to be used for self-assessments completed against systems, sites, and programs
  - Tracks security performance, testing, and accreditation progress
  - Maintains security artifacts and deliverables for the SA process
  - Tracks key information points of contact for systems, sites, and programs
  - Performs data validation
- Weakness Management
  - Tracks IT security weaknesses identified in various ways (for example, by audits and security reviews)
  - Tracks status of weakness remediation, resource allocations, and scheduled completion dates

- Access Control
  - Role and domain level access control and reporting including Executive, Department-wide, Component, Regional, and System
  - Read-only auditor access
  - Help desk access
- Reporting
  - Provides an OMB-compliant Plans of Action and Milestones (POA&M) tracking and reporting capability
  - Provides Security Performance reports
  - Privacy Sensitive Information which highlights annual privacy sensitive information performance
- Requirements Traceability Matrix (RTM)
- Security Assessment Plan (SAP)
- Security Plan (SP)
- Security Assessment Report (SAR)
- Contingency Plan
- ISSO Designation Letters
- ATO/IATO Designation Letters

Classified IACS (CIACS) is located on LAN B and is accessible by any user with HSDN or SCIF access. CIACS is classified at the SECRET level; all data for SECRET systems may be input into the tool. Those systems classified as TOP SECRET, however, are entered into CTAF by name and identification only; POA&Ms and associated SA documents for TOP SECRET systems are to be secured at the Component facility.

3.2 Management Aggregation and Security Tool (MAST)

The automated tools used by DHS ISO enable accurate system and document tracking and provide quality assurance measures. Monthly data feeds from each Component are processed and aggregated in a Continuous Monitoring Database (CMDB) within ISO MAST. This data is then used to tabulate Scorecard totals.

Data is transferred between submission method and the Management Aggregation and Security Tool (MAST) via encrypted Universal Serial Bus (USB) flash drives. Access to MAST is physically restricted to all personnel except those supporting continuous monitoring at the ISO. Once data enters MAST, it is not removed for any purpose other than to fulfill mandatory reporting requirements. Data is consolidated and normalized for report generation. It is stored on a standalone, air-gapped system. The import process does not determine nor recognize the tool used to provide the data. The application identifies based upon field names and required format. This means that any tool can be used to provide ISCM required data as long as all data elements are provided.

3.3 ISO Reporting Tool

Crystal Reports is a business intelligence application used to develop reports from a wide variety of data sources. Using direct connections to Oracle, Crystal Reports is able to obtain data from IACS and several other sources to generate daily and monthly reports. Examples of reports include:

- Security Authorization reports showing reports with expiring ATOs
- POA&M reports to show status of POA&Ms, due dates, and milestones reached
- Inventory reports of systems to include Software Development Life Cycle (SDLC) status, classification, and investment information
- Security Controls reports which display controls that have been satisfied, not started, not completed, not applicable, etc.
- Privacy Reports to show privacy sensitive systems and privacy document status
- Daily scorecard reports to show overall security compliance of component's systems.

3.4 Accessing DHS Security Management Tools

The DHS Security Management Tools are web-based and can be securely accessed from the Internet. Access to each tool site is controlled by a two-part login procedure. Requests for too access must be made through the Component Information System Security Manager (ISSM) or designated Point of Contact (POC). The following information is required to obtain an account:

- First and last name
- Email address
- Phone number
- Role Requested (e.g., ISSM, ISSO, Auditor, Privacy)
- Component

The IACS portal is located at:
http://mgmt-ocio-sp.dhs.gov/ciso/compliance/iacs/SitePages/Home.aspx

The Crystal Reports website is located at: https://dhscr.dhs.gov

Each Component is responsible for managing the accounts under its authority. The Component CISO, ISSM, or POC is responsible for ensuring that the names submitted for user accounts are valid user for access DHS IT systems and have a need-to-know.

3.5 Customer Service Center

DHS has a subject matter expert to provide assistance and help getting started with IACS. The Customer Service Center is available during normal business hours (7:00 a.m. to 5:00 p.m. EST) to answer questions regarding usage of the tool. The Customer Service Center can be reached via:

- Phone: 202-357-6100
- Email: ISOSupport@hq.dhs.gov

4.0 COMPONENT FISMA REPORTING

Each fiscal year, usually in late spring, OMB/FNR provides updated FISMA reporting guidance for both the quarterly and annual reports. The reporting requirements change on an annual basis and generally reflect the latest information security concerns. As discussed earlier, some of the data is generated based on data entered into IACS. The majority of data is acquired using various tools (Nessus, McAfee, Bigfix) during monthly scans that are part of the Continuous Monitoring data collection process. The Components have received a template designed by the ISO Continuous Monitoring team which specifies the formatting and type of data required from the data collection tools.

4.1 Annual FISMA Data Requirements

The annual FISMA data entry requirements for Components are summarized below. As of the date of publication of this document, every Component must enter system performance data directly into IACS. All other metrics are reported to the DHS OCISO via monthly data feeds.

4.1.1 System Inventory

Components must provide the following:

- The Federal Information Processing Standards (FIPS) 199 security categorization
- The number of systems at each FIPS level for Organization Operated Systems, Contractor Operated Systems and the collective number of those systems with a valid SA package

4.1.2 Asset Management

The Federal Continuous Monitoring Working Group (CMWG) has determined that Asset Management is one of the first areas where continuous monitoring needs to be developed. Organizations must first know about devices (both authorized/managed and unauthorized/unmanaged) and software before they can manage assets for configuration, vulnerabilities, and reachability. A key goal of hardware and software asset management is to identify and remove unmanaged assets before they are exploited and used to attack other assets. Asset management information each organization must provide includes:

- The total number of hardware assets that are connected to the organization's unclassified network
- The number of assets having automated capability to provide visibility at the organization's enterprise level into asset inventory information for all hardware assets
- Information on how often these automated capabilities are used and how long it takes a device discovery tool to complete the process
- The number of assets for which the organization has an automated capability to determine whether the asset is authorized and who manages it
- The number of assets for which the organization has the capability to remove any unauthorized devices and how long it would take to accomplish this
- Whether or not the organization can track the installed operating system vendor, product, version, and patch-level combination(s) in use on the assets in order to assess the number of operating system vulnerabilities present without scanning.

- Statement as to whether or not the organization has a current list of COTS general purpose applications installed on the assets and can report on the number of vulnerabilities via CPE without scanning
- The number of assets where the organization has implemented an automated capability to detect unauthorized software and block it from executing

4.1.3 Configuration Management

For each operating system and enterprise-wide COTS general purpose applications vendor, product, version, and patch-level referenced in Section 4.1.2 above, Components need to report the following:

- Whether or not an adequately secure configuration baseline has been defined
- The number of hardware assets with this software (covered by baseline if it exists)
- The percentage of applicable hardware assets for each kind of operating system software that has an automated capability to identify deviations from the approved configuration baselines and that provides visibility at the organization's enterprise level
- The frequency of deviation identification (in days)
- The percentage of network boundary devices assessed by an automated capability to ensure that they are adequately configured as intended

4.1.4 Vulnerability and Weakness Management

A key goal of vulnerability management is to make assets harder to exploit through mitigation or remediation. NIST's National Vulnerability Database identifies vulnerabilities to be addressed. For each operating system and enterprise-wide COTS general purpose applications vendor, product, version, and patch-level referenced in Section 4.1.2 above, Components need to report the following:

- Percentage of network boundary devices assessed by an an automated capability to ensure that they continue to be adequately free of vulnerabilities
- Percentage of hardware assets evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities present with visibility at the organization's enterprise level
- Provide the percentage of hardware assets identified in 4.1.2 that were evaluated using tools to assess the security of the systems and that generated output compliant with each of the following:
  - Common Vulnerabilities and Exposures (CVE)
  - Common Vulnerability Scoring System (CVSS)
  - Open Vulnerability and Assessment Language (OVAL)
- For systems in development and maintenance, what percentage identify and fix instances of common weaknesses prior to placing that version of the production code?
- For systems in production, what percentage report on configuration and vulnerability levels for hardware assets supporting those systems?

- Can the organization find SCAP compliant tools and good SCAP content?

4.1.5 Identity and Access Management

This section focuses on unprivileged and privileged network user accounts and whether or not a form of identification is either required, or allowed but not required, for login. The questions in this section are summarized as follows:

- How many unprivileged network user accounts does the organization have?
- How many privileged network user accounts does the organization have?
- For each account listed above, how many accounts:
  - Are allowed to log on with user ID and password?
  - Are allowed, but no required to log on with a non-PIV form of two factor authentication?
  - Are allowed, but not required, to log on with a two-factor PIV card?
  - Are required to log on with a non-PIV form of two-factor authentication?
  - Are required to log on with a two factor PIV card?
  - Are required to conduct PIV authentication at the user-account level?
- What is the estimated number of organzation internal systems?
- What percentage of internal system are configured for authentication for each of the following ways?
  - Allows user ID and password?
  - Allows, but does not enforce, non-PIV two factor authentication?
  - Allows, but does not enforce, two factor PIV card authentication?
  - Enforces non-PIV two factor authentication?
  - Enforces two factor PIV card for all users?
- What percentage of the organization's systems that have intergovernmental users enforce two-factor PIV card authentication for all users?
- Does your organization's Federal Identity, Credential, and Access Management (FICAM) implementation plan include an enterprise Identity and Access Management approach that system owners can leverage to adopt PIV enablement?

4.1.6 Data Protection

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. Components will need to report the following information regarding data protection:

- A breakdown of mobile asset types from the number of assets recorded in section 4.1.2. Mobile asset types include:
  - Laptop computers and notebooks

- Tablet-type computers
- BlackBerries and other smart phones
- Other cellular devices
- USB-connected devices
- Other mobile hardware assets

- The estimated number of these assets should be reported as well as the estimated number of these assets that have adequate encryption of data on the device.
- The percentage of email traffic on systems that implements FIPS 140-2 compliant encryption technologies, such as S/MIME, PGP, OpenPGP, or PKI when sending messages to the government and to the public?
- The organization will be asked to desribe its PKI Certificate Authority.

4.1.7 Boundary Protection

A key goal of boundary protection is to make assets harder for outsiders to exploit by keeping outsiders outside the network perimeter. The Trusted Internet Connection (TIC) is an Administration Priority, and the CMWG has recommended that it is among the areas where continuous monitoring needs to be developed. The Department will be required to report the following:

- TIC Access Providers need to report the percentage of TIC 1.0 and 2.0 capabilities that are implemented as well as the percentage of TICs with operational NCPS (EINSTEIN) deployment.
- Federal Civilian Agencies need to provide the percentage of external network traffic passing through a TIC and the percentage of external network/application interconnections to/from the organization's network passing through a TIC.

DHS Components will be asked to provide the following information:

- Percentage of email systems that implement sender verification technologies on outgoing messages?
- Percentage of email systems that employ sender verification technologies to detect forged messages from outside the network?
- Estimated percentage of incoming mail traffic (measured in messages) that is executed or opened in a sand box/virtual environment to determine whether or not it is malicious?
- The frequency at which the organization performs scheduled and unscheduled scans for unauthorized wireless access points?
- The number of networks with DLP/DRM at the gateway to capture outbound data leakage?
- Is the organization's internet service configured to manage filters, excess capacity, bandwidth, or provide other redundancies to limit the effects of information-flooding types of denial-of-service attacks on the organization's internal networks and internet services?

4.1.8 Incident Management

Given the persistence of attackers, and the relative ease of initiating numerous attacks, , it is reasonable to expect that some attacks will succeed. Organizations need to be able to detect anomalous activity and to protect against internal and external threats. Ideally, organizations would defend against those attacks in real time, but at a minimum it is expected that organizations 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.

To support Incident Management, reporting organizations need to provide the following information:

- The number of hardware assets on which controlled network penetration testing was performed in a manner making detection possible (e.g. on the production network through detection devices)
    - For those assets that were tested, the percentage of penetration events detected by during the test
    - The percentage of applicable events that were detected by NOC/SOC during the other scans or tests
    - The median time to detect penetrations during the test
    - The median time to take action against a penetration test (includes creation of a SEN, notification of system owner, etc.)

◦

4.1.9 Training and Education

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 adequate 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. To support this metric, reporting organizations need to provide the following information:

- The number of network users that have been provided and successfully completed cybersecurity awareness training during the Fiscal Year (Including the percentage of new users that have satisfactorily complete security awareness training before being granted network access)
- The extent to which users were given cybersecurity awareness training more frequently than annually
    - The frequency (in days) of content provisions
    - The percentage of additional content that addresses emerging threats not previously covered in annual training
    - The total number of organization-sponsored exercises designed to increase cybersecurity awareness and/or measure the effectivess of training

- The percentage of exercises that suffered no problems, or suffered problems that were addressed through training within three months
- The number of network users with significant security responsibilities
- The organization's standard for the longest acceptable amount of time between security training events for network users with significant security responsibilities
- The number of network users with significant security responsibilities who have taken security training within the organizational standard

4.1.10 Remote Access

Remote connections allow users to access the network without gaining physical access to 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.

Reporting organizations need to provide the following information:

- How many people log onto the organization's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services?
- For remote access, what percentage of people can log onto the organization's desktop LAN/WAN resources or services in each of the following ways?
  - What percentage are allowed to log on with user ID and password?
  - What percentage are allowed, but not required to log on with a non-PIV form of two factor authentication?
  - What percentage are allowed, but not required, to log on with a two-factor PIV card?
  - What percentage are required to log on with a non-PIV form of two-factor authentication?
  - What percentage are required to log on with a two factor PIV card?
  - What percentage are required to conduct PIV authentication at the user-account level?
- Estimated percentages for the following:
  - FIPS 140-2 connections using validated cryptographic modules
  - Prohibition of split-tunneling and dual-connected remote hosts where the laptop has two active connections
  - Configured to time-out after 30 minutes of inactivity
  - Scan for malware upon connection
- How many of the organizations systems are internet-accessible and are accessed by the organizations users? This excludes systems accessed through the remote access solutions covered in 10.1 and 10.2.
- What percentage of the organizatin's system that are internet-accessible and are access by user are configured for authentication in each of the following way:
  - What percentage allow user ID and password?

- What percentage allow, but do not enforce, non-PIV two factor authentication for users?
- What percentage allow but do not enforce, two factor PIV card for users?
- What percentage enforce non-PIV two factor authentication?
- What percentage enforce two factor PIV card for all users

4.1.11 Network Security Protocols

The use of Domain Name System Security Extension (DNSSEC) has been mandated at the Federal level to prevent the pirating of government domain names. GSA has ensured proper DNSSEC for the top-level domain names. Each organization is responsible for DNSSEC in sub-domain names, which are those below the top-level domain.

Reporting organizations need to provide the following information:

- The number of public facing domain names as well as the the number of DNS names signed using DNSSEC
- The percentage of second-level DNS names and their sub-domains for which all domains at and under the second level are signed
- The percentage of public-facing servers that use IPv6

4.2 Quarterly Reporting Requirements

Quarterly FISMA report data requirements for Components are outlined below. Every Component must make IACS and CDM data feed updates for the quarterly report on a monthly basis.

4.2.1 Asset Management

- Provide the total number of Agency IT assets
- Provide the number of Agency IT assets connected to the network where an automated capability provides visibility at the Agency level into asset inventory information.

4.2.2 Configuration Management

- Provide the number of Agency information technology assets where an automated capability provides visibility at the Agency level into system configuration information (e.g. comparison of Agency baselines to installed configurations).

4.2.3 Vulnerability Management

- Provide the number of Agency information technology assets where an automated capability provides visibility at the Agency level into detailed vulnerability information (CVE).

4.2.4 Identity and Access Management

- Provide the number of Agency network user accounts.
- Provide the number ofnetwork user accounts that are configured to require PIV authentication to the Agency network(s).

4.2.5 Boundary Protection

- Provide the percentage of the required TIC 1.0 capabilities that are implemented.
- Provide the percentage of TIC 2.0 Capabilities that are implementedProvide the percentage of external network capacity passing through a TIC/MTIPS.
- Provide the percentage of external connections passing through a TIC/MTIPS.

5.0 RESPONSIBILITIES

Security practitioners at each Component and Domain as well as the DHS CIO staff have responsibilities for various aspects of FISMA reporting. Specific responsibilities for POA&M development are documented in Attachment H to the *DHS 4300A Sensitive Systems Handbook*, "Plan of Action and Milestones (POA&M) Process Guide."

5.1 Chief Information Officer

The DHS CIO has the following FISMA reporting responsibilities:

- Allocate resources to support Department-wide FISMA reporting and POA&M process implementation.
- Submit quarterly FISMA reports to OMB.
- Oversee and monitor progress of POA&M implementation and remediation efforts.

5.2 Chief Information Security Officer

The DHS CISO has the following FISMA reporting responsibilities:

- Develop enterprise processes and procedures for FISMA reporting.
- Maintain an oversight program to ensure compliance with FISMA reporting requirements.
- Ensure that POA&M and FISMA data reported by Components is protected and disseminated only on a need-to-know basis.
- Verify that Component CISOs and ISSMs properly develop, implement, and manage a Component POA&Ms process.
- Verify that Component CISOs and ISSMs perform oversight of their Component's POA&M management process.
- Ensure that the DHS OIG has access to IACS as needed for scheduled reviews and audits.
- Develop the quarterly and annual FISMA reports as required.

5.3 Component Chief Information Officer

Component CIOs have the following FISMA reporting responsibilities:

- Allocate Component resources to support FISMA reporting and POA&M process implementation.
- Ensure that a Component level POA&M process is implemented and maintained.
- Oversee and monitor the progress of their Component's POA&M implementation and remediation efforts.

5.4 System Owners and Program Officials

System Owners and Program Officials have the following FISMA reporting responsibilities:

- Ensure that system performance data is entered into IACS.
- Manage development and implementation of corrective action plans for all systems and programs that support their operations and assets.

- Ensure that IT security weaknesses are prioritized.
- Ensure that funding is made available for correcting IT security weaknesses.

5.5 Component Chief Information Security Officers and Information System Security Managers

Each Component CISO and ISSM is responsible for the following FISMA reporting responsibilities:

- Implement and maintain a Component level POA&M process.
- Ensure that IT system performance metrics are entered into IACS and updated when a change in the performance metric occurs.
- Ensure that POA&M updates are submitted in IACS by the data submission deadlines and on a monthly basis.
- Review, on a quarterly basis, their Component's system POA&Ms for consistency and accuracy.
- Monitor the status of their Component's POA&Ms.

5.6 Information system Security Officers

Each Component ISSO is responsible for the following FISMA reporting responsibilities:

- Develop POA&Ms to track and manage the remediation of weaknesses for the systems under their control.
- Ensure that their POA&Ms are current and entered into the IACS on at least a monthly basis.
- Use IACS for collecting IT security program data for the periodic FISMA report.

6.0 DEPARTMENT SCORECARD

The Department Scorecard is a management level report that is published monthly and distributed to the CIO Council and the CISO Council. The Scorecard is based on data received by midnight on the last day of the month for the reporting period. The scorecard reflects OMB reporting requirements, DHS senior management priorities, and Component progress in implementing continuous monitoring requirements. The associated reports provide details of what factors influenced the scores shown to management in the FISMA Scorecard.