U.S. Department of Homeland Security

DHS Policy Directive 4300A,
"*Information Technology System Security Program, Sensitive Systems*"

Attachment E

FISMA Reporting

Version 2.0
July 29, 2022

Document Change History

Version	Date	Description
1.0	April 21, 2022	Updated by Processes and authorities Bruce Liming, FISMA Compliance
2.0	July 29, 2022	Added ISCM Waiver & Configuration Settings Management. Bruce Liming, FISMA Compliance

Contents

This page intentionally blank

1.0 INTRODUCTION

Introductory information. Briefly describe the document and perhaps the background of the program or procedures it describes.

1.1 Purpose

This document provides information for Department of Homeland Security (DHS) Components that are required to submit periodic reports in accordance with the Federal Information Security Modernization Act (FISMA) of 2014. FISMA requirements address security protections commensurate with the risk and magnitude of harm that can result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. FISMA reporting information is collected by the DHS Federal Network Resiliency (FNR) via Cyberscope.

This document also contains the CIO metrics used to assess the reported information.

1.2 Background

Office of Management and Budget (OMB) FISMA CIO metrics are organized around five functions outlined in the National Institute of Standards and Technology (NIST) “Framework for Improving Critical Infrastructure Cybersecurity” (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. These five functions are used to assess two overall objectives:

- Ensure that agencies implement the Administration’s priorities and best practices
- Provide the OMB with the performance data to monitor agencies’ progress toward implementing the Administration’s priorities, while recognizing that achieving these outcomes may not address every cyber threat, and that agencies may need to implement additional controls or pursue other initiatives to further bolster their cybersecurity.

FISMA requires that OMB oversee agencies’ progress in implementing the Act’s requirements.

OMB has charged the DHS Federal Network Resiliency (FNR) Branch with primary responsibility in the executive branch for the operational aspects of Federal agency cybersecurity required by FISMA. FNR requires quarterly and annual reporting of key metrics through the Cyberscope tool.

Following OMB guidance, DHS submits quarterly and annual FISMA reports via Cyberscope 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. The required data shows the degree of overall Department compliance with FISMA IT system metrics. The DHS FISMA reporting process relies on timely entry of data and scans by system owners and information security professionals into DHS security management tools and on submittal of monthly updates provided in the Component FISMA Data Call form on ServiceNow.

Components 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 compliance system for National Security Systems (NSS) exists and is known as Classified IACS (CIACS). CIACS is used for National Security Systems (NSS) which are those that collect, generate, process, store, display, transmit, or receive Unclassified, Confidential, or Secret National Security Information (NSI). FISMA reporting for systems classified as Sensitive Compartmentalized Information (SCI) is a responsibility of the Office of Intelligence and Analysis. The requirements for these systems are beyond the scope of this document.

1.3 References

Federal Laws

Federal Information Security Modernization Act of 2014 (FISMA), Public Law 113-283, 128 Stat 3087

E-Government Act of 2002, Public Law 107–347, 116 Stat. 2899, 44 U.S.C. 101

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).

OMB Memorandum M-16-03, “Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements”, Office of Management and Budget, M-17-25, October 30, 2015.

OMB Memorandum M-17-05, “Fiscal Year 2016 – 2017 Guidance on Federal Information Security and Privacy Management Requirements”, Office of Management and Budget, M-17-05, November 4, 2016.

OMB Memorandum M-17-25, “Reporting Guidance for Executive Order on Strengthening the Cyber security of Federal Networks and Critical Infrastructure”, Office of Management and Budget, M-12-20, October 30, 2015.

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

NIST SP 800-53, Rev 5, “Recommended Security Controls for Federal Information Systems and Organizations,” (September 2020)

Framework for Improving Critical Infrastructure Cybersecurity

Department of Homeland Security Publications

“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 quarterly and annual FISMA reports as follows:

Table 1: OMB Schedule of FISMA Reports

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

2.1 Secretary's Annual FISMA Report

Each October, the Secretary of Homeland Security is required to provide to the FNR, via the OMB Cyberscope application, a report that summarizes the Department's progress in meeting FISMA requirements. The report includes the results of annual information systems security reviews. FISMA requires that DHS report on all agency systems, including NSS, even though NSS are not included in the scope of the CIO Report**.** The DHS CIO metrics for which OCISO is responsible are derived from 3 different sources:

- Administration Priorities
- Key FISMA Metrics
- Baseline Questions

Throughout the year data is obtained using OCISO compliance tools as well as Component data calls. The responses are aggregated for all systems by Component and then entered the Cyberscope application at the Department level.

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 12 (HSPD-12) for logical access control

Although these priorities have evolved to encompass further requirements or have had requirements removed to emphasize new priorities identified as having the greatest probability of success in mitigating cybersecurity risks to agency information systems, the priorities have continued to be included in the CIO FISMA metrics.

Because Federal agencies experience persistent and increasingly sophisticated cyber threats to systems and networks containing sensitive information, the OMB and Congress took a series of aggressive actions to provide agencies with the tools necessary to detect, mitigate, and respond to cyber threats.

In FY 2015, to further protect sensitive information and assets, and improve the resilience of Federal systems and networks, the Administration initiated the President's Management Council (PMC) Cybersecurity Assessments, updated Cybersecurity Cross Agency Priority (CAP) goals, completed a 30-Day Cybersecurity Sprint, and initiated the Cybersecurity Strategy and Implementation Plan.

In FY 2016, the collection of metrics streamlined the reporting requirements into a consolidated process, organized using the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure (the Cybersecurity Framework).

The conjunction of Cybersecurity Framework and NIST's Guide for Applying the Risk Management Framework to Federal Information systems, together with associated standards and guidelines, provides DHS with a comprehensive structure for making more informed risk-based decisions and for management of cybersecurity risks across the Department.

The Secretary's Annual Report consists of the following:

- 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
- Transmittal letter from the Secretary, including a discussion of any differences between the findings of the agency CIO and the Inspector General (IG) reports
- Status of agency compliance with OMB privacy policies completed by the Senior Agency Official for Privacy (SAOP)
- Any additional documentation requested by the current FY's OMB Memorandum on FISMA Compliance Reporting

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

The Annual FISMA Report must be approved and signed by the Secretary, but if for any reason it is not signed by the submission deadline date, it can be submitted to OMB Cyberscope without signature. When the Secretary subsequently signs, it is re-submitted to OMB Cyberscope.

2.2 CIO Quarterly FISMA Report

FISMA requires that the DHS CIO provide a quarterly update on IT security performance measures to OMB. These quarterly updates are due in January, April, and July. In the 4th quarter, the report is augmented to serve as an annual report.

3.0 DHS SECURITY MANAGEMENT TOOLS

To ensure that consistent security processes and procedures are maintained throughout the Department, the DHS Office of the Chief Information Security Officer (OCISO) requires the use of the Information Assurance Compliance System (IACS), a set of Web based commercial off the shelf (COTS) security management and reporting tools. These tools enable DHS Components maintain their systems and manage the associated risks unique to their environment.

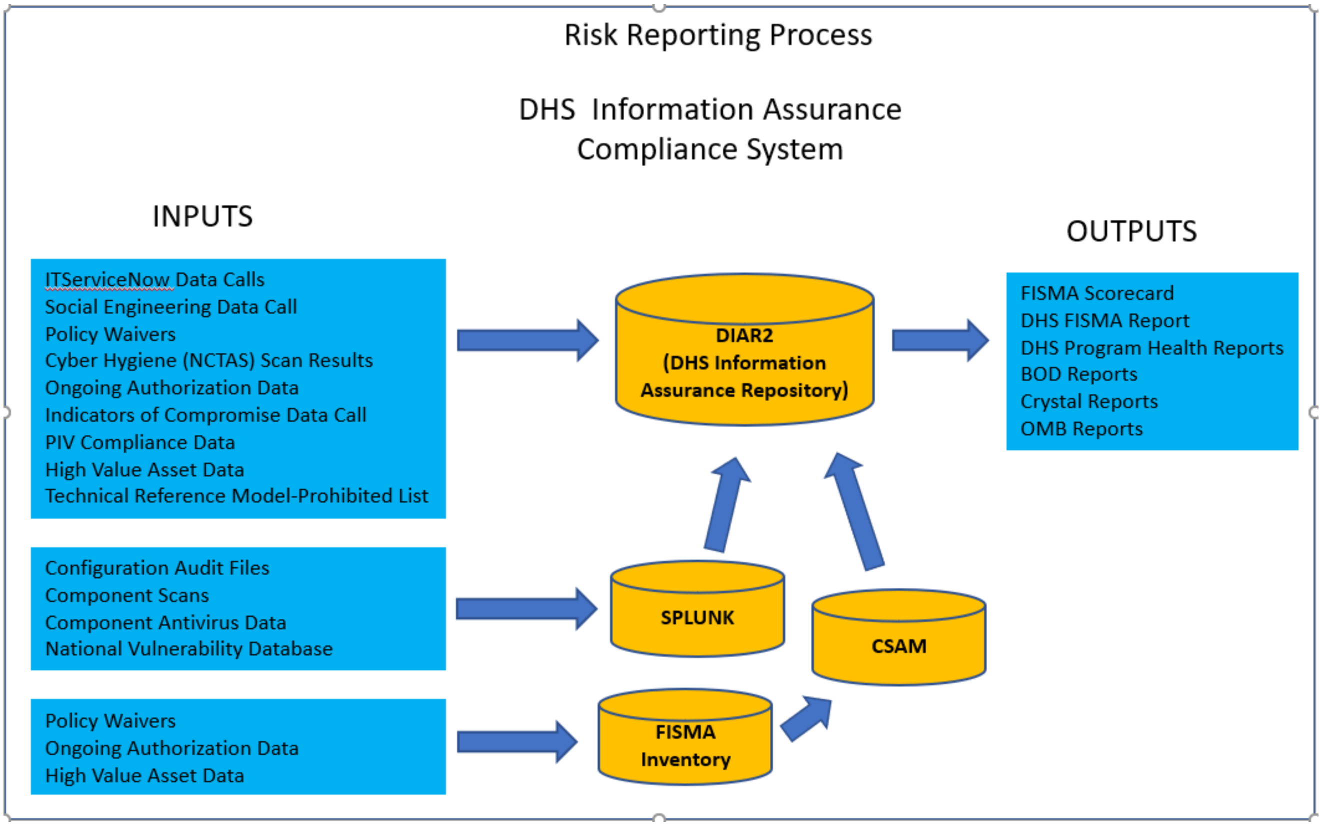
Risk Reporting Process
DHS Information Assurance Compliance System
INPUTS
OUTPUTS
ITServiceNow Data Calls
Social Engineering Data Call
Policy Waivers
Cyber Hygiene (NCTAS) Scan Results
Ongoing Authorization Data
Indicators of Compromise Data Call
PIV Compliance Data
High Value Asset Data
Technical Reference Model-Prohibited List
Configuration Audit Files
Component Scans
Component Antivirus Data
National Vulnerability Database
Policy Waivers
Ongoing Authorization Data
High Value Asset Data
DIAR2 (DHS Information Assurance Repository)
SPLUNK
CSAM
FISMA Inventory
FISMA Scorecard
DHS FISMA Report
DHS Program Health Reports
BOD Reports
Crystal Reports
OMB Reports

Figure 1: Enterprise security management tools that support FISMA

Figure 1 illustrates how the COTS enterprise security management tools in IACS: Splunk, Cyber Security Assessment and Management (CSAM), and Crystal Reports 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 reported 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 IT system data, assesses the quality of the data, and provides recommendations when necessary.

The DHS OCISO 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 OCISO 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.

The DHS FISMA compliance system, IACS, helps automate 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 following OMB requirements. IACS automates and standardizes the labor-intensive data collection and reporting processes traditionally used to gather and report FISMA data.

Data from scans (e.g., Nessus, McAfee, CrowdStrike) are submitted by the Components using .CSV files, in which data is consolidated and normalized for report generation. The import process requires certain output formats that follow a template so that the application can identify various required elements.

Cyber Security Assessment & Management (CSAM) is the Security Authorization (SA) tool for automating and standardizing portions of the SA process that assist DHS in quickly and efficiently developing security authorization packages. CSAM uses questionnaires and templates to filter a master set of DHS security requirements used to identify the subset of policies applicable to a specific IT system undergoing security authorization.

Crystal Reports is the business intelligence application used to develop reports from a wide variety of data sources. Using direct connections to the DHS Information Assurance Repository (DIAR2) database, Crystal Reports can obtain and use data from CSAM, Splunk, and other sources to generate daily, monthly, quarterly &yearly reports.

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

- Inventory Management
  - Store's 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

  - NIST Special Publication SP 800-53 security controls are used for assessments completed against systems, sites, and programs
  - Track's 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)
  - Track's 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

3.1 Accessing DHS Security Management Tools

DHS Security Management Tools can be securely accessed from the Internet. Access to each tool site is controlled by a two-part login procedure. Requests for access must be made through the Component Compliance Designee. 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 for submitting access requests online is located at: https://dhs.servicenowservices.com/ociso

Splunk is found at: https://splunk.dhs.gov

Crystal Reports is found at: https://dhscrystal.dhs.gov/BOE/BI

The CISO SharePoint Site is found at: https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso

Each Component is responsible for managing the accounts under its authority and ensuring that the names submitted for user accounts are valid users with access DHS IT systems who have a need-to-know.

3.2 Customer Service Center

DHS has a Customer Service Center to aid and help getting started with IACS/CSAM. It is available during normal business hours (7:00 a.m. to 5:00 p.m. EST) to answer questions regarding usage of the tools. The Customer Service Center can be reached via:

- Phone: 202-875-9601
- Email: dhsinfosechelpdesk@HQ.DHS.GOV

4.0 FISMA Reporting Requirements

Each fiscal year, usually in late spring, OMB and the NPPD Federal Network Resiliency (FNR) provide updated FISMA reporting guidance for both quarterly and annual reports. Reporting requirements change annually, and generally reflect the latest information security concerns. The elements consistently required for the Annual FISMA Report include the CIO Section Report, the SAOP Section Report, and the IG Section Report. After these are approved, the Secretary forwards them with a signed cover letter to the Director of OMB.

As stated earlier, some of the data for the CIO Section Report is generated from data entered into IACS. Most of the data is acquired using various tools (Nessus, McAfee, CrowdStrike, etc.) during monthly scans that are part of the Continuous Monitoring data collection process and Monthly Data Call on https://dhs.servicenowservices.com. The FISMA data call form allows Components to update their responses to FISMA questions. In addition to data collection from the tools and Components' FISMA data is gathered from the Enterprise Security Operation Center (ESOC); Identity, Credential and Access Management (ICAM); National Security Systems (NSS) Division; and Governance and Executive Management (GEM) Division.

As of the date of publication of this document, every Component must enter system performance data directly into IACS/CSAM. All other metrics are reported to the DHS OCISO via monthly data feeds or .CSV files.

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.

5.1 Secretary of the Department of Homeland Security

- Reviews the full Annual FISMA Report consisting of the CIO, SAOP, and IG FISMA Reports
- Signs the Agency letter to the Director of the Office of Management and Budget (OMB)
- Provides the Chief Information Security Officer (CISO) with the signed package and approval to submit the Department's Annual FISMA Report

5.2 Under Secretary for Management (USM)

- Reviews the FISMA Report sections provided by the Chief Information Security Officer (CIO), Senior Agency Official for Privacy (SAOP), and Inspector General (IG)
- Provides the full Annual FISMA Report consisting of the CIO, SAOP, and IG FISMA Reports to the Secretary of DHS for signature

5.3 Chief Information Officer

- Allocates resources to support Department-wide FISMA reporting and POA&M process implementation

- Provides the Annual FISMA CIO Report to the USM

5.4 Chief Information Security Officer

- Develops enterprise processes and procedures for FISMA reporting.
- Maintains an oversight program to ensure compliance with FISMA reporting requirements
- Ensures that POA&M and FISMA data reported by Components is protected and disseminated only on a need-to-know basis
- Ensures that the DHS OIG has access to IACS as needed for scheduled reviews and audits
- Develops and submits the quarterly and annual FISMA reports as required
- Provides the Annual FISMA CIO Report to the DHS CIO

5.5 Component Chief Information Officer

- Allocates Component resources to support FISMA reporting and POA&M process implementation

5.6 Component Chief Information Security Officers

- Ensures that IT system performance metrics are entered into IACS and updated when a change in the performance metric occurs
- Ensures that OCISO Data Calls are completed in a timely manner

5.7 System Owners and Program Officials

- Ensures that system performance data is properly entered in IACS
- Manages development and implementation of corrective action plans for all systems and programs that support their operations and assets
- Ensures that IT security weaknesses are prioritized and properly funded

6.0 RESPONSIBILITIES

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 Component progress in implementing FISMA requirements, other OMB reporting requirements, and DHS senior management priorities. The associated reports provide details on the factors influencing the scores shown to management in the FISMA Scorecard.

6.1 ISCM Waivers

Information Security Continuous Monitoring (ISCM) Waivers may be requested for systems that the continuous monitoring is the sole responsibility of the provider and/or corresponding authorities. All ISCM Waiver requests will be reviewed on a case-by-case basis using information from the System Security plan, CSAM, and from dialog with System Stakeholder. ISCM waiver requests require prior approval from the System Owner and Component CISO before the DHS CISOD CRMC Division will begin the review process. ISSO and ISSM approvals will not be accepted in place of System Owner and CISO approval. All documentation must be consistent and up to date. To open a ServiceNow ticket **DHS OCISO Homepage - OCISO Service Portal (servicenowservices.com).** ISCM waivers will only be considered for the following types of systems:

- Software Only (internally hosted cloud environment)
- Software as a Service (SaaS)
- FedRAMP
- Stand Alone

6.2 Configuration Management Settings

- Use the DISA STIG checks
- A chart on all related STIG checks that will be scored is located on DHS Connect Sensitive Systems Configuration Guidance (dhs.gov)