Homeland Security

OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

FY23 Information Security Performance Plan (ISPP)

Version 7.0 September 16, 2022

Approval

Kenneth Bible
Chief Information Security Officer
Office of the Chief Information Security Officer

KENNETH W BIBLE
Digitally signed by KENNETH W BIBLE
Date: 2022.09.28 11:55:42 -04'00'

Document Revision History

Version	Date	Author	Description
1.0	12/3/2021	Spencer Rothermel / Bruce Liming	Initial version posted as draft.
2.0	12/15/2021	Bruce Liming	Updated version posted as final.
3.0	1/5/2022	Bruce Liming / Lisa Minter	Updated version posted as final.
4.0	1/10/2022	Bruce Liming / Lisa Minter	Updated version sent to the CISO Council
5.0	1/18/2022	Bruce Liming / Lisa Minter	Updated with the CISO Council comments
6.0	7/28/2022	Bruce Liming / Lisa Minter	Updated to FY23
6.1	9/1/2022	Bruce Liming / Lisa Minter	Updated with Component comments
7.0	9/16/2022	Bruce Liming	FY23 ISPP Approved by the CISO Council

Contents

EXECUTIVE SUMMARY

The Annual Department of Homeland Security (DHS) Information Security Performance Plan (ISPP) defines performance requirements, priorities, and overall goals for DHS Components and the DHS Enterprise throughout the fiscal year. It is a tactical interpretation of numerous strategic inputs including Federal mandates, interagency standards, and DHS-specific policies and initiatives.

The Performance Plan deliverables provide information on security posture, compliance, and risk at the Component and Enterprise levels through an array of information security categories such as:

- Security Authorization
- Weakness Remediation

Information Security Continuous Monitoring (ISCM)

Network Operations Security Center (NOSC) threat management maturity

Other Enterprise and Chief Information Officer (CIO) initiatives

In FY23, we will continue to support all DHS Components in their efforts to meet the requirements established by the Federal Information Security Modernization Act (FISMA 2014), including renewed focus on training and collaboration, and a shift towards a more risk-focused approach. A working group session will be setup for risk reporting and new scoring methods/details based on DHS HQ/MGMT guidelines.

ISCM is a focus as DHS continues to leverage the Cybersecurity and Infrastructure Security Agency (CISA), Federal Network Resilience (FNR), and Continuous Diagnostics and Mitigation (CDM) Program to strengthen the cybersecurity of DHS networks and systems. CDM provides Federal departments and Agencies with capabilities and tools for identifying cybersecurity risks on a continuing basis, prioritizing these risks based on their potential impacts, thus enabling cybersecurity personnel to mitigate the most significant problems first. The CDM Program has bolstered capabilities and metric measurements across DHS through automated and direct-data collection, providing near real-time visibility into the “state of security” across the Enterprise.

The FY23 ISPP renews themes emphasized in previous years and enhances the effectiveness of several metrics by introducing new scoring formulas and additional details. These enhancements will promote more refined and accurate results, thereby providing a more thorough understanding of Information Security to help maintain DHS’s leadership role in the Federal Government’s cybersecurity efforts.

Please note that NSS systems are not subject to this Performance Plan. For information and guidance regarding National Security Systems (NSS), see the National Security Systems page on DHS Connect.

1.0 INTRODUCTION

1.1 Purpose

The Annual Information Security Performance Plan provides a means of improving DHS's information technology (IT) security posture by measuring compliance with policies and regulations, identifying vulnerabilities for remediation, and providing an accurate assessment of the Department's true risk posture. Performance Plan metrics track Component progress toward Departmental goals. The main product of the Performance Plan is the Information Security Monthly FISMA Scorecard. This report helps DHS stakeholders objectively compare their component performance and analyze their security and risk postures, while supporting remediation and strategic decision-making.

The FY23 ISPP continues to measure FISMA compliance in a "success-by-percentages" format focusing on the role that specific risks play within the Department, and how those risks impact the security of our information systems, networks, and devices.

The FY23 Performance Plan draws from several sources and initiatives for guidance:

Federal Cybersecurity Cross Agency Priority (CAP) Goals

Government Accountability Office (GAO) high risk priorities

Binding Operational Directives (BOD) and Policy

National Cybersecurity Assessment Technical Service (NCATS) cyber hygiene

The primary products of the requirements contained in the Performance Plan are the DHS Monthly FISMA Scorecard and supporting detailed reports. The DHS Monthly FISMA Scorecard and supporting detailed reports are used to communicate the security posture of DHS to senior executives such as the Chief Information Officer (CIO) and Chief Financial Officer (CFO) — as well as to oversee entities such as the Office of the Inspector General (OIG). Data collected may also be included in CIO FISMA reporting to the Office of Management and Budget (OMB), Federal Network Resilience (FNR), and Congress on a quarterly and annual basis.

1.2 Scope

The FY23 Performance Plan applies to all DHS Components except for the United States Coast Guard (USCG) and their reportable information systems. Reportable information systems are any General Support System (GSS) or Major Application (MAJ) with a Systems Engineering Life Cycle (SELC) of Implementation, Operational, or Modification. Components are required to maintain these systems and submit monthly scan data reflecting the security posture of their organization for analysis within the DHS Continuous Diagnostics and Mitigation (CDM) Program. These data submissions are structured around the metrics associated with overall departmental goals.

While the Performance Plan does not dictate the processes or methodology by which Components obtain the data necessary to generate these metrics, it does establish the precise type of data and format in which data must be reported, which may significantly influence collection methods. The FY23 Metrics are documented in Appendix A.

1.3 Audience

All DHS Federal employees or contractors involved in IT compliance, security, architecture, or risk management have a responsibility to be familiar with and support the goals of this Performance Plan. DHS Chief Information Security Officer Directorate (CISOD) is the owner of the Performance Plan and is responsible for managing necessary updates and modifications. The DHS CISO Council is the authorizing body for the content of the Performance Plan.

2.0 BACKGROUND

2.1 Working Groups and Integrated Project Teams

DHS chairs several working groups and Integrated Project Teams (IPTs) that serve as forums for developing and disseminating information that can help Components meet current reporting requirements and develop new capabilities for future requirements:

Chief Information Security Officer Council – The CISO Council is comprised of CISOs from each Component and meets monthly to disseminate information and solicit feedback from the Components.

Compliance Working Group (CWG) – The CWG is a forum to address all subjects related to Component FISMA operations, including Scorecard performance, FISMA Inventory, tools, and compliance related activities. This includes clarification of requirements, best practices for collecting and reporting information, and relevant changes to standard procedures.

Continuous Monitoring Working Group (CMWG) – The CMWG addresses the procurement, implementation, and operation of Enterprise ISCM solutions, and how they can best be leveraged by Components.

Information Security Training Working Group (ISTWG) – The ISTWG provides technical advice regarding the development of outreach and social engineering programs, as well as educational and training products — including, but not limited to reference documents, guides, classroom sessions, and Web-based training.

Performance Plan Working Group (PPWG) – The PPWG is responsible for reviewing current DHS Information Security FISMA Scorecard metrics and making recommendations for the next fiscal year. It is comprised of members from all Components and is led by DHS CISOD staff from the Cybersecurity Risk Management and Compliance division.

The DHS OCIO OCISO Cybersecurity Risk Management & Compliance team typically hosts symposiums twice a year for the DHS Information Risk Management and Compliance communities. A Symposium is conducted in the Fall of the upcoming fiscal year and in the Spring. ·The goals are two-fold:

1. To set the stage for the upcoming fiscal year by highlighting emerging processes and best practices.
2. To provide information and resources to IA professionals and promote networking opportunities for increased awareness and impact.

2.2 Objectives

In FY23, the Department intends to:

Continue to evaluate the DHS risk-management approach through an evolved Scorecard that supports each Component's mission requirements

Continue to mature ISCM capabilities and effectiveness across the Enterprise

Bolster collaboration to provide more efficient processes and promote Enterprise-wide security tool standardization in support of CDM

Continue to hold Component "one-on-one" meetings to foster collaboration and to provide FISMA metric updates to the components.

2.3 Strategy

In addition to representing Departmental information security initiatives, the Performance Plan supports Federal directives, congressional requirements, National Institute of Standards and Technology (NIST) guidance, Executive Orders, and CIO FISMA priorities. The FY23 metrics reports on the following activities:

Inventory of Systems and Assets – Ensuring visibility and accountability for all information systems and assets is essential to the completeness and integrity of nearly all other metrics. Inventory metrics reflect whether Department requirements are being met comprehensively

Security Management – Security Management metrics address longstanding security practices, many of which are Federal compliance requirements. This activity also addresses Ongoing Authorization (OA) efforts and how OA can more effectively use traditional Security Authorization (SA) resources, click this Link, may need to request access.

Information Security Continuous Monitoring – ISCM metrics help maintain an accurate picture of an organization's real-time security risk posture through consistent leveraging of management tools, security controls, and prioritized risk mitigation

Enterprise Solutions – Enterprise Solutions metrics are not system-specific, but instead measure the effectiveness of enterprise security initiatives deployed by both large programs and entire Components

The metrics that comprise each group are collectively used to form the DHS Information Security Monthly FISMA Scorecard that is published for all Components. More detailed reports that examine these metrics at the system and asset level are available. This tiered approach maximizes visibility into all levels of the Department's security posture.

3.0 INVENTORY

The goal of monitoring assets across the Enterprise is to ensure that each facet of an Information System is at minimum-risk. Ensuring security at the system level enhances security for the Enterprise. Systems not accounted for are at greater risk, due to the uncertainty of ownership, maintenance, and compliance with Federal mandates, directives, and policies. CSAM, the Department's compliance management system, allows for the enforcement of FISMA guidelines, as well as the ability to detect, identify, and report threats to system security.

DHS Information Assurance Compliance System (IACS) is a FISMA System that consists of three separate, web-based Enterprise applications in support of the Cybersecurity Risk Management and Compliance (CRMC) Division under the DHS CISOD: CSAM, Splunk and SAP Business Objects Crystal Reports. CSAM is DOJ's GOTS security

tool which serves as a repository to support information systems, and provides the capability to assess, document, manage, and report on the status of information technology in compliance with the Risk Management Framework. The purpose of the system is to help Agencies maintain compliance with Federal laws and policies. Functions of the tool include automated inventory, configuration, and vulnerability management and monitoring; enterprise-wide risk posture view through a heat map, which lays out the strongest and weakest areas of an organization; and experienced client engagement specialists and technical support.

Splunk is the Department's current ISCM tool. It contains numerous plug-ins or means of ingesting scan data from various vulnerability-scanning tools such as McAfee, Symantec, and Nessus. This scan data is aggregated into information that not only provides Information Systems Security Officers (ISSO) and Information System Owners (ISO) insight into their systems' overall security posture, but also provides a means for analysis and scoring against the metrics defined later in this Performance Plan.

All ISCM metric calculations rely on data available from CDM data feeds seen through Splunk. Crystal Reports provides the platform for viewing data compiled from CSAM & Splunk. Its major product is the Daily Scorecard, which provides system-level breakdowns of Component metric scores. The other reports within Crystal Reports provide asset-level details to support Components in remediation of weaknesses and gaps highlighted in the Monthly Scorecard. As a result of the shift to Splunk data sources, some reports currently available in Crystal Reports may be phased out. Any report that is removed will be replaced with Component dashboards/specific reports that can be utilized to meet reporting requirements or assist remediation activities.

The Federal Information Security Management Act (FISMA) requires DHS to develop and maintain an inventory of all information systems and assets operated by the Department. The Office of the Chief Information Security Officer (CISOD), Cybersecurity Risk Management and Compliance (CRMC) Division, is responsible for maintaining the inventory of all DHS systems and assets. This list includes all General Support Systems (GSS), Major Applications (MAJ), minor applications (MIN Approval date), subsystems (SUB), and External Information Systems (EIS). In addition, CISOD leads the inventory change control process and assists DHS Components in meeting compliance requirements for proper system categorization and reporting. The asset inventory is maintained through DHS Component scans and is stored by NOSC Splunk. The system inventory is maintained by the CISOD FISMA Inventory Management Team (IMT) in the Cyber Security Assessment and Management (CSAM) tool and can be found under reports, system general details, display. For additional information on inventory procedures and requirements, please refer to the DHS FISMA System Inventory Methodology.

3.1 System Inventory

In FY23, the priorities are to:
Implement a quarterly inventory review process with DHS Components
Develop a Cybersecurity Reciprocity Instruction to support the CIO Cybersecurity Reciprocity Memorandum
Update the DHS FISMA System Inventory Methodology
Continue engagement with the CFO and Privacy Teams to review systems identified as multi-component
Track and categorize Cloud systems (e.g., public, private, hybrid)
Charter a Control Board for major inventory changes (e.g., downgrading Major Applications to Subsystems or Minor Applications)
Manage process changes related to data migration to new Security Authorization applications for DHS Components and the Enterprise
Components will review and update their system Security Authorization data within CSAM in a timely manner
Components will submit Inventory Change Requests (ICRs) when an inventory change has occurred
Components will scan, monitor, and report all Sensitive but Unclassified (SBU) systems and assets within their boundaries to CISOD through an approved DHS tool set (Splunk or CSAM)

The CISOD IMT will discover and maintain Components' inventories of systems through the Change Request (CR) process, discovery activities, and quarterly refresh process.

3.2 HVA, MES, and CFO

New systems being added to the inventory, or existing systems that are requesting changes, may be part of a special designation of systems. These include HVA, MES, CFO-designated, and Privacy- designated systems. These systems require specialized controls and oversight, and some are weighted more heavily on the Scorecard.

3.2.1 High Value Assets

HVA refers to an asset, system, or dataset that contains sensitive data, and is used in critical operations of the Department. It also houses a unique collection of data, by size or content, that would make it of interest to attackers. A primary attribute of an HVA is the level of impact incurred by loss or compromise. If the Agency that owns the information system cannot accomplish its Primary Mission Essential Functions or is designated as having a critical function associated with maintaining the security and resilience of the Federal Civilian Enterprise, it is an HVA. To aid Components in determining if a system is an HVA, an HVA decision tool has been added to Tab 3 of the 18-02 Data Call form.

The HVA list is maintained by CISOD's CRMC Division and tracked within CyberScope as such. All Change Requests (CRs) submitted to modify a system's HVA designation must be accompanied by the Component CISO's signature. Once the CR is received by the FISMA IMT, a notification email will be sent to the DHS CISO CyberScope Point of Contact (POC). The DHS CISO CyberScope POC will review the documentation and reach out to the Component HVA POC requesting the completion of the BOD 18-02 - HVA Submission Form - Data Call. Upon receipt and completion of the HVA Submission Form, the DHS CISO CyberScope POC will upload the HVA Submission Form into CyberScope. The IMT will then update the HVA flag in CSAM in accordance with the DHS FISMA System Inventory Methodology.

To request a copy of the HVA Submission form email dhs-hvapmo@hq.dhs.gov.

3.2.2 Mission Essential Systems

Components have discretion to decide which systems to designate as Mission Essential, provided their Federal Information Processing Standards (FIPS)-199 Availability Rating is not "Low." Neither non-operational systems nor EIS may be deemed Mission Essential. All Mission Essential Systems must satisfy at least one of seven Primary Mission Essential Functions (PMEFs) listed below:

1. Secure and Manage the Borders
2. Secure Critical Infrastructure and Cyberspace
3. Protect National Leadership
4. Provide Domestic Situational Awareness
5. Enforce Homeland Security Laws and Regulations
6. Coordinate Continuity and Incident Response
7. Coordinate Disaster Recovery

Systems qualifying as Mission Essential are added to a tracking list maintained at the Enterprise

Operations Center (EOC) SharePoint Site. An accurate, up to date MES List is vital to ensuring continuity of essential operations following a calamitous event. Since the MES List is a Federal priority, Components should ensure that all systems deemed Mission Essential are identified. All MES systems are considered HVAs and must be added to CSAM and CyberScope as such. An ICR form needs to be submitted for any MES that are not designated as HVA. The ICR should either add the system as an HVA or remove the MES status.

3.2.3 Chief Financial Officer Designated Systems

DHS CFO-designated systems are systems that require additional management and accountability to ensure that effective internal controls exist over financial reporting. DHS OCFO publishes the approved list of CFO-designated systems annually. Section 3.15 of DHS Sensitive Systems Policy Directive 4300A provides additional requirements for these systems based on Appendix A to OMB Circular No. A-123, *"Management's Responsibility for Internal Control"*.

3.2.4 Privacy Designated Systems

A Privacy Sensitive System is any system that collects, uses, disseminates, or maintains personally identifiable information (PII) or Sensitive PII as recorded by the DHS Privacy Office in a Privacy Threshold Analysis (PTA).

3.3 Asset Inventory

Components are required to report all their hardware and software assets to accurately maintain a full inventory for the ISCM Program, which supports all FISMA-related activities as defined by the NIST Risk Management Framework.

A hardware asset, referred to as "asset" in this text, is defined as:

> *An addressable device that can be connected to a DHS Network or used during operational or business activities. Hardware assets include, but are not limited to, laptops, workstations, servers, virtual computing platforms, network devices, mobile devices, printers, and communications media.*

A software asset is defined as:

> *Any application, excluding an operating system, deployed on a hardware device.*

The requirements for which assets must be scanned and reported are detailed in Appendix A and are referred to as "Known Assets." Known Assets represent the entire population of a component's hardware asset inventory that should be reported via the FISMA Data Call. Known Assets that are scanned and reported to CISOD are classified as either "Managed" or "Unauthorized," depending on whether they are tied to a FISMA system boundary.

Scanned Assets serve as the scoring population for ISCM metrics and are associated with a valid FISMA Identifier (ID) and hostname. Unauthorized assets that have a hostname, but are not associated with a valid FISMA ID, reside within the 'Unauthorized' boundary. Table 1 below lists additional asset terms and definitions.

Table 1: Asset definitions

Term	Definition	Possible Implications
In-Scope Asset	A device that is or should be connected to the unclassified network and that maintains an IP address. Smartphones are included as In-Scope and report for Hardware Asset Management (HWAM) only if they are connected to an organizational internal WI-FI network.	Should be scanned for monthly ISCM reporting and will be scored for Hardware Asset Management.
Scanned Asset	Devices which have submitted scan data to CDM for the current reporting month, regardless of device type and regardless of boundary association (i.e., managed, or unauthorized).	Scanned Assets make up the scoring population for the Scorecard and can be called "Reportable Assets" (comparable to 'Reportable Systems). If an asset was scanned and the associated system boundary is not reportable (i.e., has a SELC of Development or Retired, the asset will not be reportable in Crystal Reports or on the Scorecard.
Managed Asset	A scanned asset that is linked to a valid FISMA ID and has a DNS host name.	In order to properly assign requirements to an asset, it must be managed.
Unauthorized Asset	An asset that should be scanned, has been scanned, and has a non-blank host name, but is not assigned to a FISMA ID within the scan data.	Unauthorized assets reduce the Hardware Management score.

Term	Definition	Possible Implications
Identified Assets	Servers, workstations, and laptops must have a recognized OS (operating system), i.e., not "Undetermined." Workstations and laptops cannot have an IP Address as a host name. *Servers can have an IP address as a host name.* All other assets can have an "Undetermined" OS and an IP address as a host name, if the device role is not "Unknown."	Assets must be identified to pass ISCM metrics, although not all identified assets are applicable to every metric. Certain assets (e.g., printers and network devices) that cannot report an Operating System (OS) may be considered "identified" if their device role is properly annotated in their monthly ISCM data.
Unidentified Assets	An asset that has been scanned and is linked to a valid FISMA ID but fails to meet established criteria to be considered "Identified." Assets that have an unknown device role, undetermined OS, and IP address as a host name are considered unidentified.	"Unidentified" assets fail every automated ISCM Metric, including Hardware Asset Management, Software Asset Management, Vulnerability Management, Configuration Management, and Malware Defense.
Known Assets	Total of desktops, laptops, servers, networking devices and other devices as reported on the DHS Scorecard monthly FISMA Data Call submitted by the last day of each month into the ServiceNow application once established.	Known Assets are not feeding into a metric calculation but provide a general indication of what portion of known assets are being scanned.
Invalid host name	When a workstation or laptop displays an IP address as a host name.	A laptop or workstation with an invalid hostname is classified as "Unidentified," and is entered into the CMDB. "Unidentified" assets fail every automated ISCM Metric.

4.0 INFORMATION SECURITY CONTINUOUS MONITORING

ISCM is a key priority at all Federal Agencies and provides agencies with a snapshot of the security posture of the assets in their information systems and networks and allows visibility to change in that posture over time.

ISCM is accomplished using automated security management tools that can detect, quantify, report, and potentially mitigate risks on a near real-time basis. Credentialed scans, also known as authenticated scans, are required as part of the future ISCM Strategy. The Continuous Diagnostics and Mitigation (CDM) Program will provide continuous monitoring, diagnosis, and mitigation activities designed to strengthen the security posture of the Federal.gov networks.

4.1 Existing ISCM Capability Groups and Tools

In recent years, Components managed the implementation of Enterprise Continuous Monitoring Capabilities using a variety of tools to meet the technical capabilities required for an effective ISCM Program. Standardization is encouraged by managing Enterprise License Agreements (ELA), as well as by consolidating numerous disparate contracts and licenses across the Department. Current ISCM data collection efforts (Section 5.4: ISCM Data Collection, Aggregation, and Storage) are directly aligned with Phase One of the CDM Program. Table 2 lists ISCM capability groups and tools used in the Department.

Table 2: ISCM capability groups and tools

Capability Group	Description	Current ELA Tool(s)
Asset Management	Identification of hardware and software Assets.	Tenable Nessus and/or McAfee ePolicy Orchestrator (ePO).
Network-Based Vulnerability Auditing	Credentialed vulnerability scanning achieved through periodic network scans.	Tenable Nessus and Security Center.
Configuration Management	Active detection and remediation of non-compliant configurations. Capable of making changes directly to host endpoint.	Tenable Nessus and/or McAfee ePO, Tanium & SCCM.
Endpoint Protection	Capabilities such as anti-virus, anti-malware, Host Based Intrusion Detection System (HID)s, and Host based Intrusion Protection (HIP)s.	CrowdStrike, McAfee ENS & McAfee ePO and Endpoint Protection Advanced tool suite, Tanium, Symantec & Qualys (This is not all-inclusive list).

4.2 ISCM Data

Enhancing the Security of Federal Information and Information Systems requires that agencies develop an ISCM plan and deploy Enterprise ISCM products and services instead of multiple disparate services across Agency Components. While standard Enterprise tools are available to all Components, use of these tools will not be mandatory in FY23. Nevertheless, monthly reporting standards exist, largely based on the capabilities and output formats of the standard Enterprise-tools.

The table that follows lists required data elements corresponding to each of the FY23 ISCM metrics. The data elements will change as CDM is implemented. See Appendix A for corresponding metric details about these capabilities. See https://nvd.nist.gov/general for detailed descriptions of OS, Common Vulnerability and Exposures (CVE), and Configuration Control ID standards.

Table 3: Data elements for ISCM metrics.

Capability	Requirement Data Elements
Malware Defense (Endpoint Protection)	Column Headings will be modified to better describe the contents of the data and will be moving to the CDM program for collection. • Group Notes (FISMA Name and FISMA ID) • Hostname • Last Seen (AV currency) • Last Detected Time • Host IPS
Asset Information (Applies to all ISCM metrics)	• FISMA ID • Hostname • OS Standard Name • Device Role • Last scan date • Credentialed scan (True/False)
Configuration Management	• Hostname • Configuration name/version • Configuration Control ID standard • Configuration status (pass, fail, exception)
Software Asset Management	• Hostname • OS • Application (cpe:/a) and Operating System (cpe:/o) is used for Prohibited Operating System according to the Enterprise Architecture (EA) Technical Reference Model (TRM)

Vulnerability Management	• Hostname • Common Vulnerability and Exposure (CVE) standard • Common Vulnerability Scoring System (CVSS 3.x)

Note: *Assets that do not report any ISCM data in a reporting month will not be evaluated for that reporting month.*

4.3 Continuous Diagnostics and Mitigation

The Continuous Diagnostics and Mitigation (CDM) Program provides continuous monitoring, diagnosis, and mitigation activities designed to strengthen the security posture of *.gov* networks. The CDM Program enables DHS, along with other Federal Departments and Agencies and State, local, regional, and tribal governments that can enhance and further automate their existing continuous network monitoring capabilities to correlate and analyze critical security-related information, enhancing risk-based decision-making at both the Agency and Federal Enterprise level.

It is envisioned that CDM Elastic Agency-level dashboards will empower technical managers to prioritize and mitigate risks. DHS maintains a dashboard to provide situational awareness of CDM data provided by Components to the Department, which is shared at the Federal level. DHS CISOD has begun using these resources for certain reporting requirements and will strengthen this effort as the program matures.

4.4 Transition to CDM

At the start of FY22 the Department completed the transition for ISCM data metrics collection. ISCM metric calculations rely on data available from CDM data feeds.

FY23 will see the addition of each Components CDM Agency-Wide Adaptive Risk Enumeration (AWARE) score to the Scorecard. Components Average Endpoint AWARE Total will appear on Page 2 once the algorithm provides a stable score. The AWARE calculation is comprised of various parameters tailored to measure active vulnerabilities within network boundaries. These vulnerabilities include software vulnerabilities, configuration setting management (based on DISA STIGs) and unauthorized hardware. AWARE uses a scaled CVSS score as its base and then includes factors such as age, weight, and tolerance to arrive at an overall number. A low AWARE score indicates lower overall risk, while a higher number indicates increased risk.

The Average Endpoint AWARE score is based on the component total AWARE score and divided by the number of reported assets. This metric will not be used until such time that CISA certifies the accuracy of the data and trust it with high confidence. At such a time the CISO Council will be notified, and the Average Endpoint AWARE score will be given a color rating. Specific targets will be defined at that time.

In FY23 as CDM implementation matures Hardware Asset Management, Software Asset Management, Configuration Management, Vulnerability Management, Scan Compliance and Host Based Defense calculations may change. The timeline for this transition has not been established and components will be provided notice of any changes through the year.

Additional details on AWARE scoring and the CDM program are available from CISA at https://www.cisa.gov/cdm-training. To register to receive training opportunity notices please contact CyberInsights@hq.dhs.gov

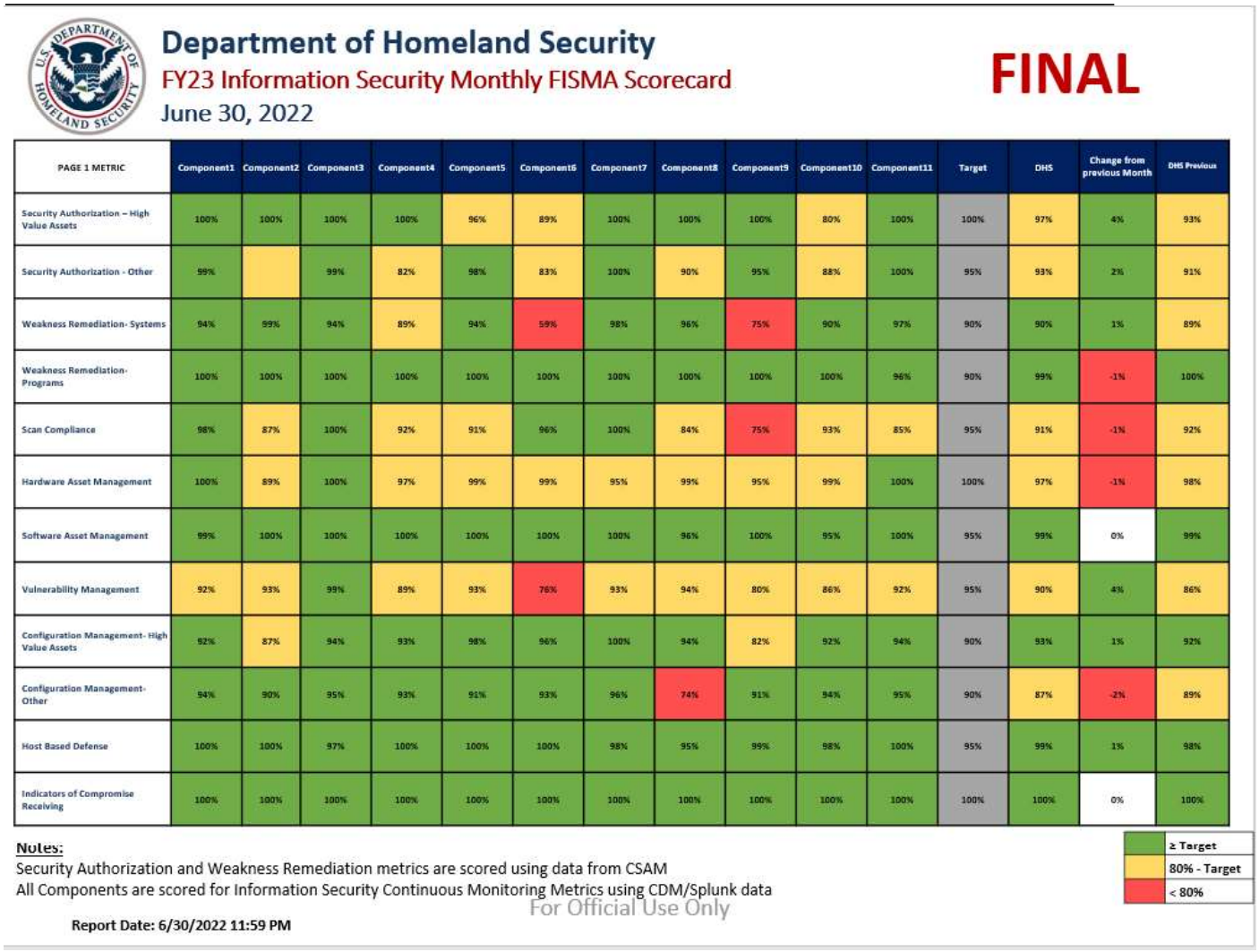
5.0 DHS INFORMATION SECURITY FISMA METRICS

The Information Security FISMA Metrics were developed with the goal of improving the accuracy of data being collected and the fairness of the scores being reported, and to provide actionable information to stakeholders for improving their compliance and overall security posture. All metrics in this document have been approved for use by the CISO Council. Any updates to metrics during the fiscal year will be managed by the Compliance Working Group (CWG) and approved by the CISO Council prior to implementation. (Will be updated when the FY23 CIO Metrics document is released)

5.1 Monthly FISMA Scorecard

The DHS Information Security Monthly FISMA Scorecard is a management-level report that is distributed to the CIO Council and the CISO Council. The purpose of the Scorecard is to provide senior management with a monthly snapshot of each Component's information security standing and the Department's security posture. Metric calculations use information sourced from CDM data feeds, CSAM, FISMA Data Calls, TRM, NOSC portal, and Cyber Hygiene scans.
Scores are based on requirements outlined in this document.

Continuing in FY23 the DHS Department score reflects an average of component scores.



Department of Homeland Security
FY23 Information Security Monthly FISMA Scorecard
June 30, 2022

FINAL

PAGE 1 METRIC	Component1	Component2	Component3	Component4	Component5	Component6	Component7	Component8	Component9	Component10	Component11	Target	DHS	Change from previous Month	DHS Previous
Security Authorization – High Value Assets	100%	100%	100%	100%	96%	89%	100%	100%	100%	80%	100%	100%	97%	4%	93%
Security Authorization - Other	99%		99%	82%	98%	83%	100%	90%	95%	88%	100%	95%	93%	2%	91%
Weakness Remediation- Systems	94%	99%	94%	89%	94%	59%	98%	96%	75%	90%	97%	90%	90%	1%	89%
Weakness Remediation- Programs	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	96%	90%	99%	-1%	100%
Scan Compliance	98%	87%	100%	92%	91%	96%	100%	84%	75%	93%	85%	95%	91%	-1%	92%
Hardware Asset Management	100%	89%	100%	97%	99%	99%	95%	99%	95%	99%	100%	100%	97%	-1%	98%
Software Asset Management	99%	100%	100%	100%	100%	100%	100%	96%	100%	95%	100%	95%	99%	0%	99%
Vulnerability Management	92%	93%	99%	89%	93%	76%	93%	94%	80%	86%	92%	95%	90%	4%	86%
Configuration Management- High Value Assets	92%	87%	94%	93%	98%	96%	100%	94%	82%	92%	94%	90%	93%	1%	92%
Configuration Management- Other	94%	90%	95%	93%	91%	93%	96%	74%	91%	94%	95%	90%	87%	-2%	89%
Host Based Defense	100%	100%	97%	100%	100%	100%	98%	95%	99%	98%	100%	95%	99%	1%	98%
Indicators of Compromise Receiving	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	0%	100%

Notes:
Security Authorization and Weakness Remediation metrics are scored using data from CSAM
All Components are scored for Information Security Continuous Monitoring Metrics using CDM/Splunk data

≥ Target
80% - Target
< 80%

For Official Use Only

Report Date: 6/30/2022 11:59 PM

Figure 1: Mockup of Monthly FISMA Scorecard

5.2 Security Management Metrics

This section describes the Security Management applicable metrics, as well as initiatives that are affecting them or are likely to affect them in the future. A significant objective is to reduce the amount of duplicative effort and cost often necessitated by the Security Authorization (SA) process. Security Management processes such as common controls, OA, and Security Plan (SP) reduction have been emphasized since FY12 to streamline the SA process for the entire Department.

5.2.1 Security Authorization

The Security Authorization (SA) process applies the Risk Management Framework (RMF) from NIST Special Publication (SP) 800-37 Rev. 2, and includes conducting the activities of security categorization, security control selection and implementation, security control assessment (Either independent or not), information system authorization, and security control monitoring. This process also helps ensure that information system management is consistent with the Department's mission, business objectives, and overall risk strategy. The process also integrates information security, including security controls, into DHS Enterprise architecture and the SELC process. It also supports consistent, well-informed security authorization decisions throughout the life cycle of

the information system.

Authority to Operate (ATO) is the official management decision given by a senior official of the organization to authorize operation of an information system, and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls. Security authorization requires the comprehensive testing and evaluation of security features (also known as controls) of an information system. Further, it addresses software and hardware security safeguards; considers procedural, physical, and personnel security measures; and establishes the extent to which a design (or architecture), configuration, and implementation meet a specified set of security requirements throughout the life cycle of the information system. Security Authorization (SA) also considers procedural, physical, and personnel security measures deployed to enforce information security DHS or Component policy.

The SA process is vital to ensuring that security procedures for all reportable DHS Systems are properly documented, validated, and updated on a regular basis. The Department currently requires that systems submit updated SA documentation to HQ CISOD for review at least every three years to obtain validation of the system's security authorization package unless the system is enrolled in the Ongoing Authorization (OA) program. HQ CISOD's CRMC Division performs a document review (DR) to verify compliance with FISMA, NIST, and DHS requirements.

Components must have a valid SA for each applicable system to remain compliant with DHS and Federal requirements. A valid SA is also a requirement of OA. To achieve a valid authorization, a system authorization package must be completed and validated through the DR process.

The SA package includes the following documents:

- Security Plan (SP)
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Contingency Plan (CP)
- Contingency Plan Test (CPT)
- Privacy Threshold Analysis (PTA)
- Privacy Impact Assessment (PIA)
- Systems of Record Notice (SORN)
- Signed Authority to Operate ATO letter

Privacy tasks are performed by the Privacy Office in each Component that has one otherwise it will be performed by the DHS Privacy Office. The "Systems Passing Privacy Checks" metric was introduced in FY19 to indicate the percent of systems that are failing Security Authorization solely due to Privacy Checks.

Per DHS Sensitive Systems Policy Directive 4300A, section 3.9.h, an ATO of six months or less also requires an ATO authorization period waiver from the DHS CISO before submission to the AO for a final authorization decision.

The DHS FISMA Monthly Scorecard Security Authorization is scored based on the following five checks:

Security Authorization Check	Requirements	Impact

Auth Status Check	Auth Date cannot be NULL and cannot be a future date. If Expiration date < current date the system will fail the Auth Status check. If Expiration date = current date system will pass.	All systems must pass this check to pass the Security Authorization metric. This is the only check required for systems with an Authority to Proceed (ATP).
DR Check	Document Review Date cannot be NULL and cannot be a future date. Date indicates DHS DR Team has approved the systems Security Authorization package.	ATO and OATO systems must pass this check to pass the Security Authorization metric.
CP Check	CP Date cannot be NULL and cannot be a future date. CP Date is based on when DHS DR Team completed its review of the CP.	ATO and OATO systems must pass this check to pass the Security Authorization metric.
CPT Check	CPT Date cannot be NULL, cannot be a future date, and must be within the past 1 year. CPT Date reflects the actual test date.	ATO and OATO systems must pass this check to pass the Security Authorization metric.
Privacy Check	PTA Date cannot be NULL, cannot be a future date, and must have a valid expiration date. (Request put in for CSAM to add expiration date.) IF PIA is Required, PIA Date cannot be NULL, and cannot be a future date. IF SORN is Required SORN date cannot be NULL and cannot be a future date.	ATO and OATO systems must pass this check to pass the Security Authorization metric.

In the Spring of FY19, DHS CISOD introduced the Authority to Proceed (ATP), which allows eligible new systems to operate on the network, prior to receiving a full ATO. Systems with a valid ATP will pass the Security Authorization metric. If a system does not receive a full ATO within one year of the ATP, the ATP becomes invalid, and the system will fail the Security Authorization metric.

5.2.1.1 Ongoing Authorization

OA is a time-driven and event-driven process whereby the Authorizing Official (AO) is provided with the near real-time security state of an information system, including the effectiveness of the

security controls deployed and inherited by the system.1 A three-year assessment cycle is not always the optimal practice, which sometimes overlooks interim changes to a System's security posture.

OA helps security officials maintain an ongoing state of awareness for their system(s), resulting in an enhanced opportunity to make more informed, risk-based decisions on the utilization of Component and System informational asset resources. Standards and processes regarding the implementation and management of OA are documented in the DHS OA Methodology document located on DHS Connect.

5.2.1.2 Document Review

Through comprehensive system document reviews, DHS CISOD ensures that systems are compliant with FISMA requirements, meet NIST and DHS control implementation standards, and are eligible for initial and continued operation. The Department's document review policy requires that system documentation be submitted whenever significant changes occur, but at least every three (3) years unless otherwise specified to obtain or maintain a valid Authorization.

5.2.1.3 Contingency Plan and Contingency Plan Tests

Over the course of the previous fiscal year, several Contingency Plans (CP) submitted did not pass initial document review. Some of the leading causes for CP failures were:

- Backup methodology not provided
- System diagram not included
- Recovery steps not adequately documented
- Lack of an Alternate Processing Site, and no POA&M or Waiver to address finding
- Activation Criteria not documented—which includes the maximum tolerable down time or other criteria before the CP can be activated
- CP not updated—Contact list (particularly, the team responsible for contingency planning) in CP document is different from personnel involved in the annual CP exercise and implemented or planned controls must match the CP/CPT documentation

[1] ***Supplemental Guidance on Ongoing Authorization, "Transitioning to Near Real-Time Risk Management", June 2014***

Below are some tips for improving the CPs prior to submitting for review:

- Backup types and frequency must be adequately documented stating that backup procedures are enforced or followed is not enough as that does not describe the frequency nor type frequency can be daily, weekly and type can be incremental, differential, and full. For Cloud systems like AWS, these are usually performed through Near Instant Replication Ensure CP documents are updated annually with attention to Personnel Listing due to transitions
- Properly document recovery procedures/recovery steps
- Create Plan of Action & Milestone (POA&M) for the lack of an alternate site or secure an approved waiver; the POA&M/waiver must be referenced in the CP document
- Document activation criteria
- Because some system/network diagrams may be too complex or large to include in the CP

document, the diagram can be uploaded and saved as an artifact in CSAM the location of the diagram must be referenced in the CP document

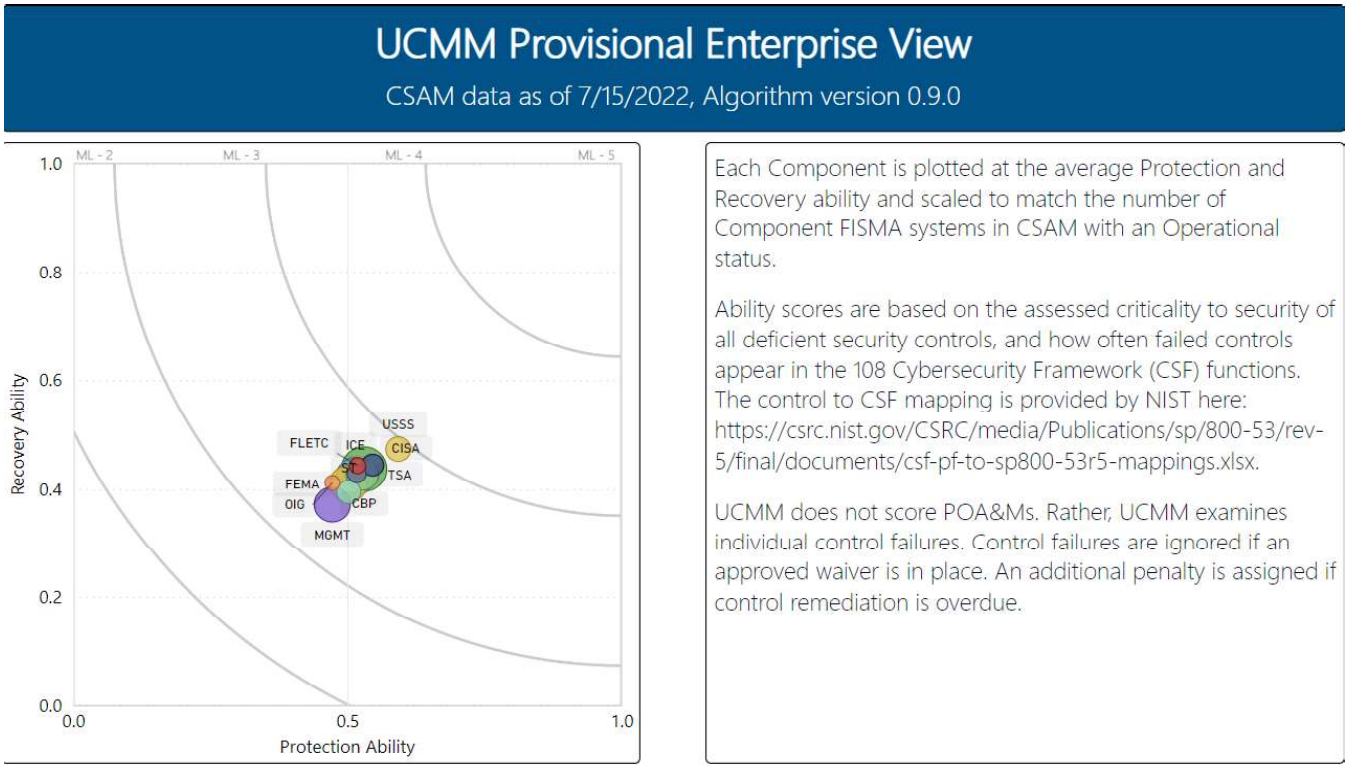
DHS CISOD will ensure roles and responsibilities of stakeholders involved in information systems contingency planning have been defined and communicated across the organization, including appropriate delegations of authority.

Standards and processes regarding the implementation and management of Document Review can be obtained Cybersecurity Risk management and Compliance.

5.2.2 Weakness Remediation

A POA&M documents the plan to remediate IT security vulnerabilities (e.g., control deficiencies), the resources required, people responsible, milestones, and planned completion dates. POA&Ms are a measure of risk since they document existing vulnerabilities in a System or Program. The Weakness Remediation metric on the DHS FISMA Scorecard measures the key aspects of POA&M quality and effectiveness. Improving the quality and effectiveness of POA&Ms across the enterprise will continue to be a major focus in FY23. Weakness Remediation – Programs scoring will not change.

In January 2023, Weakness Remediation will be updated to Unified Cybersecurity Maturity Model (UCMM) ratings. A snapshot in time as of the last full month will be used.



Program POA&Ms will remain separated into a distinct metric.

The FY23 Weakness Remediation and FY23 Weakness Remediation – Programs reports are available in Crystal Reports to provide system level detail for better tracking and remediation.

These reports reflect all applicable POA&Ms and provide details on which checks are passing or failing, and the data points associated with those checks. Weighting for POA&Ms tied to HVA systems will also remain in effect, 70% for HVA, 30% for other.

Checks for Weakness Remediation - Program POA&Ms are the same except for the Open Check: Status is In Progress/Delayed and open less than or equal 5 years.

In addition to being scored for Weakness Remediation, DHS CISOD will monitor the creation and management of POA&Ms on the completeness and accuracy of the weakness remediation progress across the Department. DHS CISOD will conduct reviews of weakness remediation progress, including the identification of new weaknesses, based on the POA&Ms in CSAM.

Possible areas of focus are:

- Funding Resources Required
- Source and Type of Funding
- Staff Resources Required
- Actual Cost
- Milestones
- Identified During
- Overall Status
- Exception/Waiver Expiration Date

Component CISO (or designated ISSM) approval is required for the status to move from Draft to In-Progress.

CRMC Division staff are available to assist Components with developing or improving POA&Ms to ensure that quality standards and scheduled completion dates are met. Components are supported through POA&M reviews, which provide feedback on whether planned corrective actions:

- Are properly captured in POA&Ms within the required timeframes
- Meet compliance criteria established in this ISPP

5.2.3 POA&M Waivers

System level POA&Ms that cannot be completed within 12 months require a DHS CISO approved waiver for non-compliance with DHS policy. POA&M waivers cover all checks for quality and timeliness and did not change in FY23. If a POA&M has a valid waiver, it will automatically pass the Weakness Remediation metric, even if multiple checks are failing. The failed checks will still be reflected on the FY22 Weakness Remediation reports in Crystal Reports but will not impact the overall passing status of the POA&M. Once the expiration date has passed, the waiver is no longer valid, and the POA&M will be subject to all quality and timeliness checks once again.

5.2.4 Risk Acceptance

POA&M exceptions are Component risk acceptance and are to be treated the same as a DHS POA&M Waiver. Reference Attachments B (Waivers and Exceptions) & H (Process Guide for Plan of Action and Milestones) of the DHS 4300A Sensitive Systems Handbook. Artifacts should be routed to iso.reporting@hq.dhs.gov.

5.3 Information Security Continuous Monitoring Metrics

The data flow for ISCM metrics begins with Component scans being imported into CISA CDM Program. A copy of that data is then sent to the NOSC and scored using enterprise Splunk dashboards.

A draft of the Scorecard will be created on the 1st or 2nd business day of the month and then shared with Component compliance POCs. Corrections will be accepted up to five days after the draft DHS Monthly FISMA Scorecard has been provided. ISCM data collection, aggregation, and storage is subject to change as the CDM Program is implemented.

5.3.1 Scanned Assets

Scanned Assets are devices which have submitted scan data to CDM/Splunk for the current reporting month, regardless of device type or boundary association (e.g., managed, or unauthorized). Scanned Assets make up the scoring population for the Scorecard, and can be called

"Reportable Assets," which are comparable to "Reportable Systems." All ISCM metrics will be based solely on data ingested for the month being reported. All assets can be connected to a DHS Network and used during operational or business activities.

> ***Pro Tip:*** If an asset was scanned, and the associated system boundary becomes non-reportable (i.e., has a SELC status changed to Retired), the asset will not be reflected in Crystal Reports or the Scorecard, only SELC statuses of implementation, modification, or operational.

5.3.2 Scan Compliance

Scan Compliance ensures that Components are scanning and reporting all systems by calculating the percentage of systems that provide scan data. Scan Compliance is calculated at the Component level by dividing the number of systems that have reported data for one or more managed assets by the sum of all systems (GSS/MAJ) that are reportable and do not have an ISCM Waiver.

5.3.3 Hardware Asset Management

Identification of assets is vital to constructing an accurate and functioning ISCM Program. Components are required to identify and report hardware and software assets monthly to CISOD. All non-dormant devices must be scanned. Any device that can be connected to a DHS Network and used during operational or business activities, should be scored if they are active on the network. Once CDM is fully implemented, information on all devices will be refreshed every 72 hours.

Hardware Asset Management will be evaluated based on the percentage of identifiable device information and roles. An asset is considered "Identified" when:

- Servers, workstations, and laptops have a recognized OS, e.g., not "Undetermined"
- Workstations and laptops cannot have IP Address as a host name

- Servers are allowed to have an IP address as a host name
- All other device roles can have an OS that is "Undetermined" as long as device role is not "Unknown"

Certain assets (e.g., printers, network devices, and communication devices) cannot report an OS, but can still be classified as "Identified" if their Device Role is properly annotated and matches the Universal Device Role list in Appendix G. Components must contact iso.reporting@hq.dhs.gov to add or update device roles. Assets that have an IP address as a host name, but report no other data, will negatively impact HWAM scores. All data uploaded into CDM/Splunk must provide accurate load files to support this management metric.

5.3.4 Software Asset Management

The CISO seeks to ensure that all software in the Enterprise is authorized via DHS Enterprise Architecture (EA) Technical Reference Model (TRM) on Mobius (https://ea.dhs.gov/mobius) or has a waiver and is not on the Federal or Agency defined "Prohibited" list. The Agency Prohibited list was created in collaboration with EA, CISOD, and the CMWG members during the second quarter of FY17. Software that is not defined in DHS Approved or Prohibited lists is considered permitted until the software can be resolved through Enterprise Architecture. If no software is returned for the asset, it will fail. Components maintain and coordinate with the Enterprise Architecture team to keep Mobius updated.

All Mobius users are automatically given read-only access. Elevated permissions to make changes can be granted to users upon approval from their supervisor and the Mobius system owner. Requests for elevated permissions or to report data quality issues may be sent to mobius@hq.dhs.gov. For content maintained outside of Mobius, requests will be directed to the appropriate content owner or data steward.

5.3.5 Vulnerability Management

Components are required to report vulnerability information for all workstations, laptops, servers, network devices, and virtual machine (Mobile device vulnerabilities are managed separately and not part of the ISCM scorecard metrics). The Vulnerability Management metric is designed to assess the true risk to the enterprise due to existing vulnerabilities. In the past, Components were scored only against critical and high CVEs associated with each asset. However Common Vulnerability Scoring System (CVSS) ratings do not always accurately depict the danger or actual hazard that a CVE presents. Attackers do not rely only on "critical" vulnerabilities to achieve their goals; some of the most widespread and devastating attacks have included multiple vulnerabilities rated "high," "medium," or even "low." In response to Binding Operational Directive (BOD) 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, assets will also be scored on CVEs published in CISAs Catalog of Known Vulnerabilities, regardless of CVSS using the Due Date which is usually at least 2 weeks after the Date Added to Catalog and will receive a 0% Vulnerability Management score.

As in the past, inability to patch a device does not exclude it from scoring. Vulnerabilities are to be reported in Security Content Automation Protocol (SCAP) compliant format (i.e., CVE with an associated CVSS score that indicates severity). Scans for all servers, workstations, and laptops must be credentialed. Those without credentialed scans will receive 0%. Any asset that exceeds 5 Critical or 10 High CVEs will receive 0% for that portion of the metric. CVEs that are not part of the CISA

(KEV) Catalog will only be scored if they were published or modified to the National Vulnerability Database (NVD) prior to the 15th of the previous month.

Each asset will be given a Total Vulnerability score comprised of a Critical Vulnerability score (weighted 50%) and a High Vulnerability score (weighted 50%). Each Critical CVE will reduce the Critical Vulnerability score by 20% (10 points). Each High CVE will reduce the High Vulnerability score by 10% (5 points).

Table 4: Vulnerability scoring calculation example

Asset	Credentialed Scan	Critical CVEs	High CVEs	Known Exploited Vulnerability	Points
Server1	TRUE	3	0	0	70
Server2	TRUE	0	6	0	70
Server3	TRUE	0	0	1	0
Switch1	FALSE	5	0	0	50
Router1	FALSE	0	10	0	50
Laptop1	TRUE	10	0	0	50
Laptop2	TRUE	0	20	0	50
Laptop3	FALSE	0	2	0	0
Laptop4	TRUE	0	0	1	0
Workstation 1	TRUE	5	10	0	0
Appliance1	FALSE	0	0	0	100
Appliance2	FALSE	0	0	0	100
Printer1	FALSE	0	10	0	50
Printer2	FALSE	0	0	0	100
TOTAL	--	--	--	--	690

Based on the information above in Table 4, the system would receive a score of 49% (690 pts / 14 managed assets = 49.3). In the table above, Laptop3 received zero points because it was not credentialed scanned. Switch1 and Router1 received points, even though they were not credentialed scanned, because only Servers, Workstations, and Laptops require a credentialed scan. Appliance1 and Printer2 were not scored because they did not perform a vulnerability scan. Server3 and Laptop4 each scored zero despite having no critical or high CVEs because they reported a Known Exploited Vulnerability.

As a reminder, in FY21 we completed the transition to CVSS 3.x scoring which implemented enhanced criteria for calculating the scores. CVEs with a CVSS of 9.0-10.0 count as Critical and CVEs with a CVSS of 7.0-8.9 count as High. Older CVEs that do not have an updated CVSS 3.x score listed on the National Vulnerability Database (NVD) will be scored using the CVSS 2.x version.

CVSS v3.0 Severity Ratings	Base Score Range
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Table 5: Base score ranges for CVSS v3.0 ratings

5.3.6 Configuration Management

Like Vulnerability Management, each asset is assigned a Configuration Score. The Asset Configuration scores are summed and divided by the number of applicable assets to create the system and Component level scores.

To provide consistent reporting across all Components, DHS CISOD is providing SCAP-based audit files for all configuration applicable Operating Systems. Only tests included in DHS provided audit files will count towards the Configuration Management score. The available audit files can be found on DHS Connect at: https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx The DHS CISO may issue updated and revised configuration standards.

Asset Configuration Scores are based on the weighted percentages of CAT I 50%, CAT II 30% and CAT III 20% of SCAP checks passed. HVA and non-HVA systems will be reported separately.

The OS determines applicability to the Configuration Management metric. In FY23 the number of OS being scored will expand to include Red Hat Enterprise Linux (RHEL) 8, Ubuntu 18 & 20 and CENTOS 7.

To receive credit, Components must submit the specific SV (Rule ID) or WN (STIG ID) for each check that was performed, and the result of each test. If the expected checks are not present, missing checks will count as failed checks. Checks that return "error" or "warning" will not count as failed. If the unique environment of a system prevents some CAT I - III checks from completing accurately. Please email the DHS FISMA Scorecard Team dhshqcontinuousmonitoring@hq.dhs.gov. A meeting will be scheduled to discuss the specific issues and, if necessary, authorize a modification to the audit file for limited use, for False/Positive results.

Components are still required to report configuration information for OS where DHS audit baselines have not been published, though they will not be scored at this time. In the absence of DHS published baselines, Components are encouraged to use Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). If neither DHS nor DISA guidance is available, Components should utilize other authorized benchmarks or industry or

vendor best practices.

Note: The OS determines applicability to the Configuration Management metric; however, assets with the device role 'appliance' are not evaluated. Please refer to the Universal Device Role List for more information.

5.3.7 Host Based Defense

Components must demonstrate progress in implementing endpoint protection measures by reporting whether antivirus capabilities are installed, active and up to date on applicable endpoints (or hosts) and Host Intrusion Prevention System (HIPS) is enabled on all endpoints. Endpoints are defined as workstations, laptops, and servers.

Anti-Virus (AV) definition files must be updated within 15 days of the last scan date for the asset to pass; however, it is recommended best practice to update daily. The last scan date is equal to the last time the asset was scanned, regardless of scan type. Components are encouraged to submit the AV Product Number to receive accurate credit for AV. HIPS capability must be installed and active on each endpoint. HIPs values that allow assets to pass are 'ENABLED,' 'GREEN,' 'HOST IPS ENABLED,' 'ON,' 'ONLINE,' 'TRUE,' 'YES,' and '1.'

The weighting for this metric will be split evenly, 50/50, for both AV and HIPS. All assets submitting ISCM scan data in the current month, that excludes AV/HIPS, will receive a Host Based Defense score of 0%. Likewise, if an asset reports AV or HIPS data, but no other ISCM data, the asset with score 0% for all other ISCM metrics. If no ISCM data is reported for an asset in the current month, it is excluded from scoring.

For Components using CrowdStrike since there is not a definition file the Anti-Virus (AV) definition file date will be the last time the Policy was checked which usually results with the same date/time of the Last Detected Time. The plan is to automate and possibly move to the CDM program for collection.

Table 7: Sample AV submission

Group Notes	System Name	DAT Version (VirusScan Enterprise)	Last Detected Time	Host IPS Status (Host IPS)
Fuel Management Initiative DHQ-12345-MAJ-12345	Server1	4/1/2021 0:00	4/15/2021 0:00	Enabled

5.3.8 Prohibited OS

Prohibited OS reflects the number of OS's found in component scan data that are currently listed as "Prohibited" via DHS Enterprise Architecture (EA) Technical Reference Model (TRM) on Mobius (https://ea.dhs.gov/mobius). OS is evaluated using the Component level TRM. If the OS is not listed at the Component level, the Enterprise level will be used. If the OS is not listed on either the Component or Enterprise level, it will count as Prohibited.

Users may request updates to the TRM or report data quality issues by contacting mobius@hq.dhs.gov .

5.3.9 Indicators of Compromise (IOC) Receiving

This metric ensures that Components are receiving Unclassified IOCs, can determine if the IOC is impacting their environment and are able to perform an enterprise search for the IOC. This metric supports establishing and maintaining baseline cyber health for DHS. Capabilities include

determining where in the Intrusion Defense Chain (IDC) the event occurred, the source of the infection, the time to implement countermeasures, the location in the IDC where countermeasures are implemented, and the time to report to NOSC.

The test is conducted monthly by the DHS Network Operations Security Center (NOSC), and components are scored on three phases:

1. Acknowledgement on C-LAN
2. Acknowledgement on A-LAN
3. Reporting Host Sweep results using the IOC Tracker

Components will receive credit based on how quickly they are able to respond. Full Credit (100%) will be awarded for acknowledging within 24 hours of original notification. Partial Credit (50%) will be awarded for acknowledging after 24 hours. If no acknowledgment is received, the score for that phase will be 0%. Points are awarded for each phase; Green, 100; Yellow, 50; Red, 0. Each phase represents a third of the final IOC score.

5.3.10 FY23 CIO FISMA Reporting and EO 14028

FISMA requires agencies to report the status of their information security programs to OMB and requires Inspectors General (IG) to conduct annual independent assessments of those programs. OMB and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) collaborate with interagency partners to develop the Chief Information Officer (CIO) FISMA metrics.

In response to EO 14028 *Improving the Nation's Cybersecurity*, several new metrics have been added to quarterly CIO FISMA Reporting. While these are new quarterly reporting requirements, a subset of these new metrics will also be reported on the DHS Monthly Scorecard. The metrics below are examples of what may be reported on the DHS Monthly FISMA Scorecard for FY22. **(Will be updated when the FY23 CIO Metrics document is released).**

MFA and Encryption (2.1) How many systems encrypt sensitive data at rest? (NIST SP 800-53 r4 SC-28). The data source is the quarterly data call.

Logging (3.1) Using the model defined in OMB M-21-31, provide a self-evaluation of the maturity of the agency's enterprise log management capability.

a) Tier IL0 Not effective - Logging requirements focused on highest criticality are either not performed or partially performed
b) Tier IL1 Basic - Logging requirements only focused on highest criticality are performed
c) Tier IL2 Intermediate - Logging requirements focused on highest and intermediate criticality are performed
d) Tier IL3 Advanced - Logging requirements at all criticality levels are performed

Critical Software (4.0) Number of instances of on-premises critical software, defined in Definition of Critical Software under Executive Order (EO) 14028, at the agency.

Implementing IPv6 (5.1) Number of Government Furnished Equipment (GFE) hardware assets (from 1.2.1-1.2.3) that are fully running IPv6.

Vulnerability Disclosure (9.1) What is the status of the agency's Vulnerability Disclosure Program (VDP), per OMB M-20-32, Improving Vulnerability Identification, Management, and Remediation.

a) Established, with all internet-accessible systems in scope
b) Established, with incomplete scope or other issues (provide clarification in text)
c) Not established, in progress (provide estimated date of establishment)
d) No current plans to establish a VDP (provide a detailed rationale)

5.3.11 Social Engineering

Metrics – General Population

Components must conduct quarterly social engineering exercises based on metrics and requirements listed below. One hundred percent of each Components' general population (which also includes privileged users) must be tested according to the following metrics: Effectiveness Metrics:

#	Metric Type	Proposed Measurement	Reasoning
1	Execution (Yes or No)	Pass/Fail	Did Components conduct quarterly phishing exercises to assess the effectiveness of their training?
2	Execution (Percent of Population)	Red / Yellow / Green 0-49% / 50-99% / 100%	Components must test 100% of their userbase on a quarterly basis.
3	Effectiveness (Click Rate)	Changes per quarter – see "Complexity - Thresholds of Success" **Metric for red/yellow/green changes by quarter based on expected level of complexity.	Based on the "Complexity - Thresholds of Success", the percentage of recipients who click on a phishing link inside the email will help determine if training is successful and effective.
4	Complexity	Q1/Q2 = Moderate Q3/Q4 = High	Link to NIST Phish Scale[1]

Complexity – Thresholds of Success

Metrics 3 and 4 are broken down into the following and are based on the NIST Phish Scale:

Quarter 1	Quarter 2	Quarter 3	Quarter 4
Complexity: MODERATE	Complexity: MODERATE	Complexity: HIGH	Complexity: HIGH
CLICK RATE OF: 25% or less = GREEN 26%-35% = YELLOW	CLICK RATE OF: 25% or less = GREEN 26%-35% = YELLOW	CLICK RATE OF: 35% or less = GREEN 36%-50% =YELLOW	CLICK RATE OF: 35% or less = GREEN 36%-50% = YELLOW

>35% = RED	>35% = RED	> 50% = RED	>50% = RED

Reporting Results:

For users who click on a phishing link, they should be directed to supplemental training. Results are to be collected and submitted to OCIOSecurityTraining@hq.dhs.gov, quarterly:

FY23 dates will be provided once they become available.

Required Information Includes: Component, Did Component Conduct Phishing Exercise? (Yes/No), Date of Phishing Exercise, Total Number of Userbase, Number of Users Tested (% of Population), Click Rate (% of userbase who clicked on the phishing exercise), Complexity of Test (Low, Low-Moderate, Moderate, High).

Note: DHS can only provide guidance, each Component has a different mission, target audience, and tolerance level of content.

5.4 ISCM Data Collection, Aggregation, and Storage

Most data used for ISCM metrics begins with raw scans imported into the CDM/Splunk repository. The data is pulled overnight to DHS Information Assurance Compliance System (DIAR2) database where it is presented to Crystal Reports.

5.5 ISCM Waivers

This section has been moved to the 4300A Attachment E

5.6 Daily Reports

CISOD has made several reports available in Crystal Reports that can be run at any time to provide insight into how a system or component is scoring on a particular metric. The reports most used are the Daily FISMA Scorecard, Security Authorization and Weakness Remediation reports. The Security Authorization and Weakness Remediation reports have been updated to align with the data available in CSAM. A complete matrix for these reports is available in the appendix.

Splunk reports are automated emails that go out daily overnight. There are nine Reports per System and ten per Component.

- Configuration Settings Management (HVA & Other Component level)
- Configuration Settings Management Details
- Host Based Defense (Component level)
- Hardware Asset Management (Component level)
- Prohibited Operating System (Component level)
- Software Asset Management (Component level)
- Scanned Assets (Component level)
- Vulnerability Management (Component level)
- Vulnerability Management Details

- Scan Compliance (Component level Only)
- Indicators Of Compromise (Component level Only)

NOTE: This is based on staff and technical availability.

These system level reports give details of the Information Security and Continuous Monitoring data and can assist Components in managing compliance and remediation efforts.

If a report is not available, or a customized report is needed, a request may be submitted to ISO.Reporting@hq.dhs.gov.

5.6.1 Timing Considerations

When viewing reports in Crystal Reports, it is important to understand that the information displayed is not in real-time. Areas of Crystal Reports that are updated with information from CSAM, (e.g., Security Authorization and Weakness Remediation) are updated every two hours from 5:00 am through 5:00 pm. The interface with CDM/Splunk for ISCM metrics executes once per day, after regular business hours.

Manual data collections, such as the Monthly FISMA Data Call, are only imported into DIAR2 at the end of the scoring period and should be entered by each Component onto this SharePoint Site https://mgmt-ocio-sp.dhs.gov/ciso/CRMC/FSMBranch/DHSSupport/FISMAScorecard/SitePages/Home.aspx. Information entered on the data call form will not be visible on external reports until the end of the month.

When transitioning from one month to another, the interface with CDM/Splunk is paused until the final snapshot for the reporting month is taken. Any new data processed will not be visible until the switch to the new reporting cycle is complete. When viewing the Daily Scorecard, the lower right corner will display the "Data Captured as of" date and time (Figure 8). This represents the last run of the interface between Crystal Reports and CSAM. Below that will be the date and time the last Splunk/DIAR2 interface ran.

Note: The reporting month will show at the top of the page.

Figure 8: Daily Scorecard--the date and time stamp for last data capture and continuous monitoring run.

6.0 CIO FISMA REPORTING METRICS

6.1 FY22 Updates to CIO FISMA Reporting Metrics

In response to Executive Order 14028, OMB/CISA are updating CIO FISMA Metrics for FY22. Due to late issuing of official metrics from OMB, we are unable to publish guidance at this time.

6.2 CIO FISMA Background

The Federal Information Security Modernization Act (FISMA) of 2014 (PL 113-283, 44 USC 3554) requires the head of each Federal agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Additionally, FISMA requires agency heads to report on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise.

The Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) have a joint role in overseeing the information security programs of the Federal enterprise. OMB issues an annual FISMA guidance document which covers requirements for agency cybersecurity reporting, OMB M-21-02, Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements (FISMA Guidance). The CIO FISMA reporting metrics focus on assessing Agencies' progress toward achieving outcomes that strengthen Federal cybersecurity and assess Agency progress by:

- Ensuring that Agencies implement the Administration's priorities and best practices
- Providing the Office of Management and Budget (OMB) with the performance data to monitor Agencies' progress toward implementing the Administration's priorities

Since achieving these outcomes may not address every cyber threat, Agencies may have to implement additional controls, or pursue other initiatives to overcome their cybersecurity risks.

Since FY2016, OMB and DHS have organized the CIO FISMA metrics around the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). The FISMA metrics use the Cybersecurity Framework as a standard for managing and reducing cybersecurity risks. They are organized around the framework's five functions: Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework, when used in conjunction with NIST's Special Publication (SP) 800-37 Rev 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, and associated standards and guidelines, provides Agencies a comprehensive structure for making more informed, risk-based decisions, as well as managing cybersecurity risks across their Enterprise IISCM.

6.3 FISMA Reporting Data Calls

Due to the depth and breadth of information that is covered in the annual requirements, time constraints, and to ensure that the data collected is valid and has integrity, CISOD will track all Annual FISMA requirements throughout the fiscal year. Users who support data collection or submission efforts will need to be approved by the Component's CISO or designee to receive appropriate permissions. For permissions, send a request to the DHS InfoSec Customer Service Center at DHSinfosechelpdesk@hq.dhs.gov, together with any required approvals.

This table will be updated when the FY23 CIO Metrics document is released.

Table 5: Annual and Quarterly CIO FISMA Reporting Deadlines

Reporting Period	Component Reporting Deadline	Cyber Scope Deadline	Responsible Parties
FY23 Annual CIO, IG, SAOP FISMA Reporting	TBD	TBD	All Agencies
FY23 Q1 CIO FISMA Reporting	TBD	TBD	CFO Act Agencies

FY23 Q2 CIO FISMA Reporting	TBD	TBD	All Agencies
FY23 Q3 CIO FISMA Reporting	TBD	TBD	CFO Act Agencies
FY23 Annual CIO, IG, and SAOP FISMA Reporting	TBD	TBD	All Agencies

6.4 FISMA CIO Metrics vs DHS Information Security FISMA Metrics

The Chief Information Officer (CIO) FISMA metrics are different from the DHS Information Security FISMA Metrics. The former, track and measure Components according to the requirements adopted by FNR and report these metrics through Quarterly and Annual FISMA Reporting mechanisms. The latter were developed by CISOD through the PPWG and CISO Council meetings and are used for internal reporting. There may be times when the Monthly Scorecard includes same or similar metrics to those reported by CIO FISMA. This can raise awareness of lagging metrics, increase monitoring, and permit tracking of progress towards CIO FISMA goals.

7.0 BINDING OPERATIONAL DIRECTIVES

A binding operational directive is a compulsory direction to federal, executive branch, departments, and agencies for purposes of safeguarding federal information and information systems. The Department of Homeland Security (DHS) develops and oversees the implementation of binding operational directives pursuant to the Federal Information Security Modernization Act of 2014.

DHS binding operational directives do not apply to neither statutorily defined "National Security Systems" nor to certain systems operated by the Department of Defense or the Intelligence Community.

As new BODs are issued, additional metrics may be added to the Scorecard supplemental page to assist leadership with tracking progress in these areas.

7.1 BOD 22-01, Reducing the Significant Risk of Known Exploited Vulnerabilities

The goal of BOD 22-01 is to enable federal agencies, as well as public and private sector organizations, to improve their vulnerability management practices and dramatically reduce their exposure to cyberattacks. BOD 22-01 establishes a CISA managed catalog of known exploited vulnerabilities and requires federal civilian agencies to identify and remediate these vulnerabilities on their information systems. CISA will update this catalog with additional exploited vulnerabilities as they become known, subject to an executive level CISA review and when they satisfy the following thresholds:

- The vulnerability has an assigned Common Vulnerabilities and Exposures (CVE) ID
- There is reliable evidence that the vulnerability has been actively exploited in the wild
- There is a clear remediation action for the vulnerability, such as a vendor provided update

The Catalog of Known Exploited Vulnerabilities can be found here- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

7.2 BOD 18-01

Federal agency "cyber hygiene" greatly impacts user security. By implementing specific security standards that have been widely adopted in industry, federal agencies can ensure the integrity and confidentiality of internet-delivered data, minimize spam, and better protect users who might otherwise fall victim to a phishing email that appears to come from a government-owned system. Based on current network scan data and a clear potential for harm, this directive requires actions related to two topics: email security and web security.

All agencies are required to:

1. Develop and provide to DHS an "Agency Plan of Action for BOD 18-01" to:
   - **a.** Enhance email security by:
     - i. Configuring:
       - All internet-facing mail servers to offer STARTTLS
       - All second-level agency domains to have valid SPF/DMARC records, with at minimum a DMARC policy of "p=none" and at least one address defined as a recipient of aggregate and/or failure reports
     - ii. Ensuring:
       - Secure Sockets Layer (SSL)v2 and SSLv3 are disabled on mail servers, and
       - 3DES and RC4 ciphers are disabled on mail servers (see temporary policy exception for 3DES)
     - iii. Add the NCCIC as a recipient of DMARC aggregate reports.
     - iv. Set a DMARC policy of "reject" for all second-level domains and mail-sending hosts.
   - **b.** Enhance web security by:
     - i. Ensuring:
       - All publicly accessible Federal websites and web services provide service through a secure connection (HTTPS-only, with HSTS)
       - SSLv2 and SSLv3 are disabled on web servers
       - 3DES and RC4 ciphers are disabled on web servers
       - Identifying and providing a list to DHS of agency second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all subdomains
2. Begin implementing the plan.
3. Provide a report to DHS on the status of that implementation. Continue to report every 30 calendar days thereafter until implementation of the agency's BOD 18-01 plan is complete.

   DHS will review each Agency Plan of Action for BOD 18-01 upon receipt and contact agencies with any concerns.

   - DHS will coordinate agency-provided lists of domains for HSTS preloading with Dot Gov
   - DHS will rely on its National Cybersecurity Assessments & Technical Services team scanning for tracking and verifying progress
   - DHS will notify agencies when the NCCIC establishes a central location for the collection

of agencies DMARC aggregate reports, described above at II(1)(a)(iii).

- DHS will provide additional guidance through a DHS BOD coordination call and other engagements and products following the issuance of this directive.

7.3 BOD 18-02

To ensure effective identification and timely remediation of major and critical weaknesses to HVA systems based on DHS HVA assessments, all Federal agencies shall complete Actions One and Two; and Federal agencies selected by the Office of Management and Budget (OMB) and DHS for HVA assessments shall complete all the following actions:

- Action One - Identify and Submit Coordination Points of Contact (POCs) for HVA Assessments
- Action Two - Submit Agency HVAs
- Action Three - Participate in DHS-led Assessments
- Action Four - Ensure Timely Remediation of Identified Vulnerabilities and Report Mitigation Plans and Progress

DHS will centrally manage Agency progress and report submissions and will engage each Agency Head in all cases where the Agency has not met the deadlines outlined in Required Actions defined above. Additional details can be found at https://cyber.dhs.gov/bod/18-02/

8.0 CISOD GENERAL SUPPORT

The CISOD provides targeted support for any Component or employee requiring assistance regarding use of the FISMA tools, training material, assistance with reports and metrics, working groups, and requirements. The DHS InfoSec Customer Service Center can be reached at DHSinfosechelpdesk@hq.dhs.gov.

8.1 Outreach and Training

The CISOD CRMC Division offers Components diverse outlets for training and education, collaborative working groups, and communications channels. In FY18, CISOD began developing comprehensive outreach programs to assist Components with Compliance and Department initiatives. These Component one-on-one meetings form the backbone of CISOD's commitment to ensuring that all Information Security compliance stakeholders are informed on the current direction of the compliance program, that internal collaboration is strengthened, and that stakeholder awareness is enhanced.

Components may request assistance visits to provide training or other assistance on specific topics or scorecard-related issues (e.g., POA&Ms, Common Controls, and ISCM) via ServiceNow or email to DHSinfosechelpdesk@hq.dhs.gov.

8.2 Security Training

Because DHS employees and contractors are both its greatest strength and its greatest vulnerability, it is CISOD policy that employees undergo Annual Cybersecurity Awareness training and Annual Privileged User training, as appropriate. It is up to each Component to ensure that the training satisfies all areas of concern for the targeted audience. As the Department moves toward a

standardized training approach, review of frequency and training requirements may change to be applicable across the Enterprise.

8.2.1 Annual Privacy Training

In FY22 DHS CISOD began to report on compliance with Annual Privacy training requirements. A new metric was added to the page 2-supplemental page of the scorecard to show the percent of users compliant with Annual Privacy training requirements.

8.2.2 Privileged User Training

In addition to general Cybersecurity Awareness training, users occupying roles with privileged network access, as well as others with significant security responsibilities, must receive annual specialized training specific to their security responsibilities.

A user with significant security responsibilities (i.e., privileged user) is defined by CISOD as: "personnel, contractors, or others working on behalf of DHS (e.g., employees, detailers, military)" assigned organizationally defined roles that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include key management, account management, network and system administration, incident management, database administration, and web administration. Privileged users constitute those performing security-relevant functions at all levels (e.g., enterprise architecture, network, and information system) within the Enterprise."

Privileged users should be reminded of the risk they may face or pose to the Department due to their escalated roles. Privileged User training goes beyond basic Cybersecurity Awareness training content and focuses on the consequences of inappropriate actions or relaxed attention to security controls. Components needing to develop specialized training materials for privileged staff may use resources already provided at DHS HQ. Training submissions will be tracked via ServiceNow using the FISMA Data Call form.

9.0 SMALL UNMANNED AIRCRAFT SYSTEMS (SUAS)

In accordance with Policy Memorandum 119-08, Addressing Cybersecurity Vulnerabilities of Small Unmanned Aircraft Systems, waivers may be granted for the continued use of Small Unmanned Aircraft Systems (sUAS) and procurement of sUAS that have not been tested and deemed secure by the Department of Defense (DoD).

The Office of the Chief Information Officer (OCIO) is responsible for the establishment, administration of the waiver process, and the signature authority on all waiver recommendations. Component CISO's are responsible for ensuring all sUAS Programs meet and adhere to the requirements in both the DUSM Memo 119-08, OCIO Memorandum "Interim Policy Memorandum: Securing DHS Small Unmanned Aircraft Systems (sUAS), and this sUAS Cybersecurity Waiver Process document.

9.1 sUAS Cybersecurity Procedures

Each Component CISO is responsible for ensuring all applicable sUAS are incorporated in the DHS HQ Cyber Security Assessment and Management (CSAM). There should be a sUAS Federal Information Security Management Act (FISMA) ID assigned or a FISMA ID will be created upon a

designation of a sUAS Program.

Prior to a waiver submittal, the program must be approved by DHS Chief Readiness Support Office (CRSO). To receive approval, please contact CRSO.

Components shall document and provide to FISMA.Inventory@hq.dhs.gov their inventory and authorization information for sUAS as follows:

1. A detailed inventory of their sUAS assets.
2. If applicable, the FISMA boundary the sUAS are part of.
3. The boundary, if not part of an existing FISMA boundary, that the sUAS assets should be part of, if necessary, submitting an Information Change Request (ICR) for creation of a new system.
4. Supporting artifacts for authorization of use of the sUAS (ATO letter, authorized-use memo, and SSP, CONOPS, etc.).
5. In accordance with FISMA and 4300A requirements, the Program must implement the minimum defined security controls (Section 5.0), conduct risk assessments, and must be assessed and authorized.

Upon waiver approval by the Chief Information Officer (CIO), the Component CISO must add each sUAS to CSAM and ensure that the sUAS inventory within CSAM is the same as the applicable CRSO sUAS asset inventory.

10.0 CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT

Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of Information and Communication Technology (ICT) (including the Internet of Things) product and service supply chains. C-SCRM covers the entire life cycle of ICT, and encompasses hardware, software, and information assurance (IA), along with traditional supply chain management and supply chain security considerations. C-SCRM is the program and set of processes DHS will implement to safeguard against threats to the DHS ICT Supply Chain.

10.1 Working Groups and Integrated Project Teams

DHS Cyber – Supply Chain Risk Management Working Group (C-SCRM WG): The DHS C- SCRM WG supports the implementation of the 'Agency Requirements' as identified in Title II Federal Acquisition Supply Chain Security Act (FASCSA) of 2018. This DHS C-SCRM WG scope focuses on the establishment of the cyber supply chain initiatives as follows: Governance through a DHS Enterprise C-SCRM Program Management Office; Execute DHS Enterprise C-SCRM Policies & Procedures; Provide DHS C-SCRM Education, Training & Awareness; and Report DHS Enterprise C-SCRM Metrics & Measurements of Performance.

10.2 Objectives:

Develop C-SCRM capabilities to ensure the DHS network and related (ICT) systems and services through its entire lifecycle are composed of secure hardware, software, and services.

10.3 DHS C-SCRM Program

DHS missions are threatened by a range of potential cyber-related threats from ICT products entering operational service via the Department's supply chains. The DHS C-SCRM Program is consistent with NIST guidance and focuses on aspects of supply chain security that are more pertinent to DHS threats to our networks and missions. In some cases, DHS Contractors are exposed to the same cyber threats as the Department. To help minimize and mitigate these threats, DHS OCIO will insert C-SCRM best practices into DHS processes in a way that minimizes changes to these processes as well as minimizes the resources needed to carry out the DHS C-SCRM Program.

The DHS C-SCRM Program has coordinated with the Business Management Office Directorate (BMOD) to develop C-SCRM questions and Statemen of Work (SOW) language for the Information Technology Acquisition Review (ITAR) process.

10.4 Executing C-SCRM Across the DHS Enterprise

In DHS, C-SCRM activities are needed at all levels: from operators to small organizational entities, to functional activities, to Components, and to the DHS staff and networks in use. DHS C-SCRM activities will occur at multiple levels across DHS Headquarters (HQ), Components and Programs, and will include training to support these activities, a governance process to ensure a holistic approach to C-SCRM within DHS, and information sharing across the Enterprise. A complete set of activities and their definitions may be provided, please contact NSSCYBER@hq.dhs.gov.

C-SCRM activities should not be done in isolation from core ICT procurement and management processes executed across the Enterprise. Rather, C-SCRM should be integrated in these processes across the organization. Consistent with NIST recommended best practices for integrating C-SCRM into government organizations, DHS will establish a C-SCRM program that will be responsible for:

- Integrating C-SCRM across the Enterprise
- Coordinating DHS C-SCRM activities across the Enterprise when required
- Assisting stakeholders tasked with executing C-SCRM activities when specialized C-SCRM knowledge is required
- Assessing and monitoring C-SCRM activities to ensure that DHS follows U.S. law and DHS policy
- Developing Department-wide C-SCRM plans to ensure the security and integrity of the DHS supply chain

10.5 Organizational Responsibilities

DHS C-SCRM responsibilities and authorities exist at all levels. At the DHS Enterprise level, the DHS CIO is the senior official designated for ICT supply chain oversight and the representative to the FASC. The DHS Secretary is responsible for federal supply chain activities on behalf of all civilian agencies. The DHS C-SCRM PMO will support the DHS CIO on DHS C-SCRM matters and as it relates to FASC-related C-SCRM responsibilities.

10.5.1 Office Responsibility

Cyber Supply Chain Risk Management Program Management Office (C-SCRM PMO)

- Responsible for implementing the programs necessary to align DHS's IT personnel, resources, and assets
- Provides DHS and its Components with the IT services required to lead a unified DHS effort to prevent and deter adversarial attacks
- Cybersecurity and Infrastructure Security Agency (CISA) builds capacity to defend against cyber-attacks; works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks
- Coordinate's security and resilience efforts using trusted partnerships across the private and public sectors

Federal Acquisition Security Council (FASC)

- Sets supply chain risk management standards and manages government-wide supply chain risk activities

Office of Intelligence & Analysis (I&A)

- Integrates intelligence into operations across DHS Components, its partners in state and local government and the private sector to identify, mitigate and respond to threats

Joint Requirements Council (JRC)

- Governs Joint Requirements Integration and Management System (JRIMS) execution to enhance operational effectiveness
- Builds Component Requirements capacity and capability to provide Department-wide expertise and enhance collaboration

Management Directorate (MGMT)

- Responsible for budget, appropriations, expenditure of funds, accounting, and finance; procurement; human resources and personnel; information technology systems; biometric identification services; facilities, property, equipment, and other material resources; and identification and tracking of performance measurements relating to the responsibilities of the Department

Office of the Chief Financial Officer (OCFO)

- Oversees all financial management activities relating to the programs and operations of the agency; develops and maintains an integrated agency accounting and financial management system, including financial reporting and internal controls

Office of the Chief Procurement Officer (OCPO)

- Serves as innovative and flexible business advisors delivering the right solutions to enable the DHS mission

Office of the Chief Readiness Support Office (OCRSO)

- Responsible for facilities, sustainability and environmental programs, and assets and logistics

Office of the Chief Security Officer (OCSO)

- Delivers Enterprise-wide security solutions to protect the Department's people, information, and resources against constant evolving threats

Office of the Chief Technology Officer (OCTO)

- Streamlines the data governance efforts of the Department and removing barriers to data sharing and advanced data analytics

Office of the General Counsel (OGC)

- Responsible for Department's legal determinations and for overseeing all its attorneys

Office of Selective Acquisitions (OSA)

- Supports Classified acquisitions

Office of Program Accountability and Risk Management (PARM)

- Oversees program governance and acquisition policy
- Builds acquisition and program management capabilities
- Assesses the health of major acquisitions and investments

Science & Technology Directorate (S&T)

- Enables effective, efficient, and secure operations across all homeland security missions by applying scientific, engineering, analytic, and innovative approaches to deliver timely solutions and support departmental acquisitions

10.6 DHS C-SCRM Management Directive

10.6.1 The Under Secretary for Management:

- Determines if C-SCRM related Federal Acquisition Regulation provisions have been incorporated at the appropriate milestones in the DHS acquisition lifecycle
- Develops procedures as the department's Chief Acquisition Officer, in coordination with the Chief Information Officer, to make joint recommendations with the Chief Information Officer to the Secretary regarding exclusion and removal orders and implements such orders directed by the Secretary per (A) in section III of this policy

10.6.2 The Chief Information Officer:

- Serves as the senior official responsible for C-SCRM within DHS and coordinates with other senior federal agency officials on C-SCRM efforts
- Performs those functions assigned by law, executive order, regulation, departmental policy, or delegated by the Secretary of Homeland Security to implement the DHS C-SCRM

program and related requirements, such as congressional notifications and reporting
- Represents the department on the Federal Acquisition Security Council (FASC) and is responsible for implementing FASC guidance pertinent to DHS as necessary
- Oversees the DHS C-SCRM program management office (PMO) and DHS Enterprise C-SCRM Working Group
- Oversees the development of DHS Enterprise-level C-SCRM processes and procedures for DHS Information and Communications Technology (ICT) major acquisition programs (as defined in DHS Management Directive 102-01), products (e.g., hardware systems, devices, and software), and services (e.g., telecommunication services, helpdesk or IT support services, cloud computing and storage services)
- Monitors the DHS network to identify C-SCRM risks
- Operates and maintains necessary capabilities to support C-SCRM risk decisions
- Oversees the development and promulgation departmental training to relevant personnel for key C-SCRM activities
- Develops and monitors departmental performance metrics and C-SCRM assessments and manages internal and external reporting requirements
- Performs necessary reviews, including Committee on Foreign Investment in the United States (CFIUS) reviews, reviews of C-SCRM requirements for ICT major acquisition programs, C-SCRM reviews for ICT products and services (i.e., product assessments), threat and criticality assessments and vendor due-diligence assessments for ICT major acquisition programs, products, services, and vendors
- Reviews and approves or rejects waiver requests for covered ICT products and services
- Develops, implements, and maintains necessary data storage

10.6.3 Component Heads:

- Implement departmental C-SCRM guidance
- Develop/update and implement Component specific C-SCRM policies, processes, and procedures consistent with departmental guidance
- Develop/update, implement, and monitor Component C-SCRM related training, including policies, guidelines, and best practices, for Component personnel consistent with direction from the DHS C-SCRM PMO
- Oversees, through the Component Acquisition Executive, Component compliance with C-SCRM related acquisition requirements and processes
- Ensure Component participation as needed in departmental C-SCRM Working Group activities
- Report information on departmental C-SCRM metrics and C-SCRM assessments to the DHS C-SCRM PMO
- Develop Component specific performance metrics, C-SCRM assessments, and reporting processes consistent with departmental guidance
- Provide relevant information to support departmental C-SCRM activities as requested by

the DHS C-SCRM PM

11.0 FISMA REPORTING DATA CALLS

Due to the depth and breadth of information that is covered in the annual requirements, time constraints, and to ensure that the data collected is valid and has integrity CISOD will track all Annual FISMA requirements throughout the fiscal year. Presently the FISMA Reporting SharePoint site is used for monthly DHS Scorecard reporting. Users who support data collection or submission efforts will need to be approved by the Component's CISO or designee to receive appropriate permissions. For permissions, send a request to the DHS InfoSec Customer Service Center at DHSinfosechelpdesk@hq.dhs.gov, together with any required approvals. In FY23 the plan is to develop the FISMA Quarterly data call in SharePoint.

APPENDIX A: DHS MONTHLY FISMA SCORECARD PAGE 1 METRICS

The DHS FY23 Monthly FISMA Scorecard translates metric scores into percentages ranging from 0% to 100%, where a higher percentage indicates greater compliance.

The tables throughout this appendix list, describe, and provide target scores for each Scorecard metric.

Metric	Description	FY22 Target
Security Authorization – HVA	% of SBU Reportable HVA systems meeting valid authorization requirements.	100%
Security Authorization – Other	% of SBU Reportable systems not listed as HVA which meet valid authorization requirements.	95%
Weakness Remediation – Program	% of POA&Ms for Programs meeting quality checks and specified timelines (not incomplete, overdue, or delayed) as listed in the current ISPP.	90%
Scan Compliance	% of reportable systems submitting scan data during the current reporting month. Excludes systems with approved waivers.	95%
Hardware Asset Management	% of assets with identifiable device information and roles.	100%
SW Asset Management	% of applicable assets that are not running prohibited software. If no software is identified, the asset will fail.	95%
Vulnerability Management	Evaluates system vulnerability by scoring asset CVEs against the established thresholds. Servers, workstation, and laptop scans must be credentialed.	95%

Configuration Management – HVA	% of applicable HVA assets meeting and passing required configuration checks. Applicability is based upon OS, with certain device roles being excluded.	90%
Configuration Management – Other	% of applicable non-HVA assets meeting and passing required configuration checks. Applicability is based upon OS, with certain device roles being excluded.	90%
Host Based Defense	% of assets meeting endpoint security requirements such that a) anti-virus is installed and current and b) Host Intrusion Protection (HIPS) is installed and enabled. Anti-Virus software must be updated within 15 days from the last scan date for every endpoint. For Components using CrowdStrike since there is not a definition file the Anti-Virus (AV) definition file date will be the last time the Policy was checked which usually results with the same date/time of the Last Detected Time.	95%
Indicators of Compromise	% of capability to receive an IOC and perform enterprise-wide sweeps for them.	100%

A.1 Security Authorization HVA

Detail	Description
Metric Name	Security Authorization – HVA
Metric Type	Effectiveness
Purpose	DHS seeks to reduce the number of systems with invalid or out-of-date Authorization packages. HVA systems approved for OA will also be included in this metric.
Data Source	CSAM
Reporting Frequency	Every 2 hours from 5:00 a.m. - 5:00 p.m.
Responsible Parties	ISSO, ISO, AO, and Compliance Team

Special Conditions	Systems applicable for evaluation are GSS and MAJ listed in CISOD's FISMA inventory with a status of Operational, Implementation, or Modification. An ATO will be entered into CSAM after the DR Team approval. Ongoing Authorization: • Must additionally have completed the OA Checklist, OA Admission Letter, and have published the Control Allocation Table within the past 3 years published in CSAM when available. • Ongoing Authorization Eligibility Task must be complete and approved by the ISSO, ISSM, and DHS OA Team when available. • Must complete an Annual CPT like all other systems.

Detail	Description

Description	Percentage (%) of SBU reportable HVA systems meeting valid authorization requirements.
	
	Non- Ongoing Authorization Systems – the following must be valid:
	• Approval Date valid
	  ○ [ATO Approval Date is ATO Decision date (if after 3/1/2017) or DR approval date
	  ○ If Accreditation Date <= Current date minus 3 months (must have 3 months of ISCM data in good standing) and (Accreditation Date < 11/01/2013 or ATO Approval Date > Accreditation Date minus 3 months]
	• ATO – Component
	• CP – DHS Document Review
	• CPT – DHS Document Review
	• SAR – DHS Document Review
	• SP – DHS Document Review
	• SAP – DHS Document Review
	• PTA – Privacy (every 3 years)
	• PIA – Privacy (if applicable)
	• SORN – Privacy (if applicable)
	Ongoing Authorization Systems – the following must be valid:
	• CPT – DHS Document Review
	• PTA – Privacy (every 3 years)
	• PIA – Privacy PIA/SORN
	• SORN – Privacy PIA/SORN
	• Annual Control Testing of approved CAT- Component

Target	100%
Metric Calculation	Number of reportable HVA systems meeting all Security Authorization checks divided by total number of reportable HVA systems.
Crystal Reports	FY23 Daily Scorecard FY23 Security Authorization • Component • System Name • FISMAID • HVA • CFO • Auth Type • Security Authorization Status • Auth Status Check • DR Check • CP Check

Detail	Description
	• CPT Check • Privacy Check • Auth Date • Auth Expiration • Document Review Date • CPR Date • CPT Date • PTA Valid • PTA Date • PIA Valid • PIA Required • PIA Date • SORN Valid • SORN Required • SORN Date
C&A Support	CANDA@hq.dhs.gov
Inventory Support	FISMA.Inventory@hq.dhs.gov
FAQ	Q: Why is my system failing? A: Check the FY22 Security Authorization report in Crystal Reports. That report will point to the specific check that caused the system to fail. Q: I have a signed ATO, why is my system failing? A: Systems require more than an ATO to pass Security Authorization. Check the FY22 Security Authorization report in Crystal Reports. That report will point to the specific check that caused the system to fail. Q: Why does my ATO date say 1971? A: 1971 is a default date used when the actual date is invalid. Check CSAM to ensure the ATO dates are correctly entered in the tool. Q: Why is this system showing on the scorecard, it is in development? A: Only systems with SELC of Implementation, Operational, or Modification are reported on the Scorecard. If the system is reporting in error, please contact the FISMA Inventory Management Team (IMT) and check the SELC status. If a change is required, an Inventory Change Request (ICR) form needs to be completed and sent to the IMT.

A.2 Security Authorization-Other

Detail	Description
Metric Name	Security Authorization – Other
Metric Type	Effectiveness
Purpose	DHS seeks to reduce the number of systems with invalid or out-of-date Authorization packages. HVA systems approved for OA will also be included in this metric.
Data Source	CSAM
Reporting Frequency	Every 2 hours from 5:00 a.m. - 5:00 p.m.
Responsible Parties	ISSO, ISO, AO, and Compliance Team
Special Conditions	Systems to be evaluated are GSS and MAJ listed in CISOD's FISMA inventory with a status of Operational, Implementation, or Modification. An ATO will be entered into CSAM after the DR Team approval. Ongoing Authorization: • Must additionally have completed the OA Checklist, OA Admission Letter, and have published the Control Allocation Table within the past 3 years. • Ongoing Authorization Eligibility Task must be completed and approved by the ISSO, ISSM, and DHS OA Team. • Must complete an Annual CPT • Systems with a valid Authority to Proceed (ATP) have 1 year to obtain a full ATO, or they will fail Security Authorization.

Description	% of SBU reportable systems not listed as HVA which meet valid authorization requirements (to include a new check verifying annual review of CFO key controls for CFO-designated systems — which will be incorporated in near future). Non-Ongoing Authorization Systems – the following must be valid: • Approval Date valid • [ATO Approval Date is ATO Decision date (if after 3/1/2017) or DR approval date • If Accreditation Date <= Current date minus 3 months and (Accreditation Date < 11/01/2013 or ATO Approval Date > Accreditation Date minus 3 months] • ATO – Component • CP – DHS Document Review • CPT – DHS Document Review • SAR – DHS Document Review • SP – DHS Document Review • SAP – DHS Document Review • PTA – Privacy (every 3 years) • PIA – Privacy (if applicable) • SORN – Privacy (if applicable) Ongoing Authorization Systems – the following must be valid: • CPT – DHS Document Review • PTA – Privacy (every 3 years) • PIA – Privacy PIA/SORN • SORN – Privacy PIA/SORN • Annual Self-Assessment– Component • CAT Published - Component Authority to Proceed (ATP) systems - the following must be valid: • Subset of required controls have been implemented and assessed • Component CISO Approval • DHS CISO Approval • Does not have an overall Critical/High Risk Level. • SELC of Implementation • Refer to OA or System Inventory Methodologies if needed o CFO Designated o Privacy Sensitive

Detail	Description
	○ High-Value Asset (HVA)/Mission Essential Systems (MES) ○ Contractor Owned/Managed ○ Publicly Accessible ○ External Information Systems
Target	95%
Metric Calculation	Number of other reportable systems meeting Security Authorization checks divided by total number of other reportable systems.

Detail	Description
Crystal Reports	FY23 Daily Scorecard FY23 Security Authorization • Component • System Name • FISMAID • HVA • CFO • Auth Type • Security Authorization Status • Auth Status Check • DR Check • CP Check • CPT Check • Privacy Check • Auth Date • Auth Expiration • Document Review Date • CPR Date • CPT Date • PTA Valid • PTA Date • PIA Valid • PIA Required • PIA Date • SORN Valid • SORN Required • SORN Date
C&A Support	CANDA@hq.dhs.gov
Inventory Support	FISMA.Inventory@HQ.DHS.GOV

Detail	Description
FAQ	Q: Why is my system failing? A: Check the FY23 Security Authorization report in Crystal Reports. That report will point to the specific check that caused the system to fail. Q: I have a signed ATO, why is my system failing? A: Systems require more than an ATO to pass Security Authorization. Check the FY23 Security Authorization report in Crystal Reports. That report will point to the specific check that caused the system to fail. Q: Why does my ATO date say 1971? A: 1971 is a default date that is used when the actual date is invalid. Check CSAM to ensure that the ATO dates are correctly entered in the tool. Q: This system is in development. Why is it showing on the Scorecard? A: Only systems with SELC of Implementation, Operational, or Modification are reported on the Scorecard. If the system is reporting in error, please contact the FISMA Inventory Management Team (IMT) and check the SELC status. If a change is required, an Inventory Change Request (ICR) form needs to be completed and sent to the IMT.

A.3 UCMM Maturity Level (ML)

Updates TBD once more information is provided

Detail	Description
Metric	Maturity Level 1-5
Purpose	This metric will be replacing the Weakness Remediation – Systems and Weakness Remediation - Program metric remains the same.

A.4 Weakness Remediation- Program

Detail	Description
Metric	Weakness Remediation- Program
Metric Type	Quality and Effectiveness
Purpose	Focus will be on mitigating vulnerabilities and improving management of POA&Ms.
Data Source	CSAM
Reporting Frequency	Every 2 hours from 5:00 a.m. - 5:00 p.m.

Responsible Parties	Information System Owner
Special Conditions	Only scores Open POA&Ms or POA&Ms completed within the current reporting month, or previous 11 reporting months. Beginning June 2020, if status is still OPEN after Scheduled Completion Date has passed, the POA&M will no longer fail
	Each NIST Control test failure that does not have a POA&M created within 30 days will count as a Failed POA&M. This check will only impact failures detected since the start of FY20 (October 1, 2019) Program POA&Ms may be open for up to five years, but otherwise must pass the checks listed in Appendix C.
Description	% of POA&Ms meeting quality checks and specified timelines. POA&Ms must meet the following requirements to pass: • POA&M Status Check: POA&M cannot have Status of "Not Started" if POA&M Workflow Status is "POA&M Auto Approved" • POA&M Open Check: POA&M must be open less than 5 years from Creation Date OR have a Policy Waiver AND waiver expiration date not reached • Scheduled Completion Check: Scheduled completion date is not 'null' AND Number of days between creation date and scheduled completion date must be less than or equal to 365 days (1 year) • Criticality Check (previously the Severity Check): POA&Ms must have a User Defined Criticality of Very High, High, Medium, Low or Very Low selected; Cannot be Null/ Not Selected • Identified During Check: Item Identified During cannot be Null/Not Selected • Milestone Check: Must have at least 2 milestones • POC Check: 'Assigned to' cannot be 'null'
Target	90%
Metric Calculation	[(% of HVA POA&Ms passing quality checks and timelines x 0.7) + (% of Other POA&Ms passing quality checks and timeliness x 0.3)]
Crystal Reports	FY23 Daily Scorecard FY23 Weakness Remediation (Excel Data-Only) • Component • System Name • FISMAID • WR Applicable • HVA • CFO • CSAM POA&M ID • POA&M Number

Detail	Description
	• POA&M Passing • POA&M Status Check • POA&M Open Check • Scheduled Completion Check • Criticality Check • Severity Level Check • Control Link Check • Identified During Check • Milestone Check • POC Check • POA&M Status • Workflow Status • Create Date • Scheduled Completion Date • Actual Finish Date • Days Overdue • Policy Waiver • Policy Waiver Expiration • Criticality • Severity • Controls • Item Identified During • Number of Milestones • Assigned To • Information System Owner • POA&M Title • Weakness • Risk Accepted • SELC Status • FISMA Reportable
POA&M Support	DHSinfosechelpdesk@HQ.DHS.GOV
FAQ	TBD

A.5 Scan Compliance

Detail	Description
Metric	Scan Compliance
Metric Type	Informational/ Effectiveness
Purpose	Validate every System has scan data that does not have a ISCM Waiver.

Detail	Description
Data Source	CDM/Splunk
Reporting Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, ISSMs, Compliance Teams
Special Conditions	System with an ISCM Waiver will be removed from scoring.
Description	% of the reportable FISMA Systems submitting scan data during the current reporting month OR have a valid ISCM wavier
Target	95%
Metric Calculation	# of FISMA Systems providing scan data to CDM / total # of applicable FISMA Systems. Applicable systems are the number of SBU reportable systems minus the number of systems with an approved ISCM waiver.
Splunk Reports	ScanCompliance
Scan Compliance Support	dhsinfosechelpdesk@HQ.DHS.GOV
FAQ	N/A

A.6 Hardware Asset Management

Detail	Description
Metric	Hardware Asset Management
Metric Type	Effectiveness
Purpose	Facilitate constant and comprehensive asset visibility and an automated DHS Asset Inventory. Use Continuous Monitoring tools to identify every Asset on the network and link it to an approved FISMA system.
Data Source	CDM/Splunk
Reporting Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	None
Description	% of assets with identifiable device information and roles An asset is considered “Identified” when one of the following conditions are met: An asset is considered “Identified” when:

Detail	Description
	• Servers, Workstations, and Laptops have a recognized OS, i.e., not "Undetermined." • Workstations and Laptops can NOT have IP Address as a host name. Note: Servers can have an IP address as a host name. • All other Device roles can have an OS that is "Undetermined" if device role is not "Unknown." Note: Assets not assigned to a FISMA system will count against this score. If a device role cannot be determined per APPENDIX F: UNIVERSAL DEVICE ROLE LIST, Components must contact iso.reporting@hq.dhs.gov to add or update device roles.
Target	100%
Metric Calculation	[(identified Assets / managed Assets * 100) – Unauthorized Assets %] rounded down instead of up Note: Unauthorized Assets % = (Number of Assets in Unauthorized Boundary / Total scanned assets).
Splunk Reports	Hardware Asset Management (HWAM)
Hardware Asset Management Support	dhsinfosechelpdesk@HQ.DHS.GOV
FAQ	Q: Why does it matter that every asset has a device role assigned? A: Provides evidence Components are actively managing hardware assets.

A.7 Software Asset Management

Detail	Description
Metric	Software Asset Management
Metric Type	Implementation
Purpose	To build a software asset inventory to better understand what applications are deployed on the DHS Networks and where they are deployed.
Data Source	CDM/Splunk

Detail	Description
Reporting Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	If no software is returned, the asset will fail.
Description	% of applicable assets (as listed on Universal Device Role list that are not running prohibited software). Common Platform Enumeration (CPE) CPE:/a data from the scan data is used. CISOD will evaluate applicable assets against the Component-level Technical Reference Model (TRM) Prohibited lists in Mobius. If no software is returned, the asset will fail. Note: Applicable assets not reporting software will count against this score.
Target	95%
Metric Calculation	# of Applicable Assets Reporting Non-Prohibited Software / Total # of Applicable Assets
Splunk Reports	Software Asset Management (SWAM)
Software Asset Management Support	dhsinfosechelpdesk@HQ.DHS.GOV
FAQ	Q: Why is my asset failing? There is no prohibited software. A: Assets will also fail if no software is provided.

A.8 Vulnerability Management

Detail	Description
Metric	Vulnerability Management
Metric Type	Effectiveness
Purpose	This metric is to drive remediation efforts across the Department to eliminate Critical and High vulnerabilities and raise more awareness of the vulnerabilities residing across the Department including those that reside on assets that are unable to be patched.
Data Source	CDM/Splunk
Reporting Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams

Special Conditions	Servers, Workstations, and Laptops must be credentialed scanned to receive credit. For scoring purposes, CVEs with a CVSS of 9.0- 10.0 will count as Critical. CVEs with a CVSS of 7.0-8.9 will count as High. Any asset that returns CVEs is considered applicable, regardless of device role. Assets that have vulnerabilities, but remain under the threshold, will be docked for each vulnerability. • Each Critical CVE will reduce the Critical Vulnerability score (weighted 50%) by 10 percentage points. • Each High CVE will reduce the High Vulnerability score (weighted 50%) by 5 percentage points. • The total # of points, divided by # of assets, is the Total Vulnerability Score. • Properly scanned assets that report zero CVEs will receive full credit. Any asset that reports a Known Exploited Vulnerability will receive 0% for the entire metric, using the Due Date which is usually at least 2 weeks after the Date Added to Catalog. Assets cannot receive negative scores. If they exceed the CVE count threshold, they receive 0%. Any asset that returns CVEs is considered applicable, regardless of device role. CVEs published or updated to the National Vulnerability Database (NVD) after the 15th of the previous reporting month are not considered when assessing Critical or High vulnerabilities. Known Exploited Vulnerability will receive 0% for the entire metric, using the Due Date which is usually at least 2 weeks after the Date Added.
Description	Evaluates system vulnerability by scoring asset CVEs against the established thresholds. Servers, workstation, and laptop scans must be credentialed.
Target	95%
Metric Calculation	No vulnerability scan or non-credentialed scan for S/W/L = 0% If properly scanned: 1) Total VUL asset score = Critical VUL asset score + High VUL asset score. If a KEV is found, then the score is reduced to 0%.

Detail	Description
	Critical VUL asset score = [(5 - # of Critical CVEs*) / 5] x 0.5 High VUL asset score = [(10 - # of High CVEs*) / 10] x 0.5 2) Component and System Level Calculation: Sum all Total VUL asset score / # Managed Assets (assets tied to FISMA boundary) Assets cannot receive negative scores, if they exceed the CVE count threshold, they receive 0%.
Splunk Reports	VULN
Vulnerability Support	TBD
Vulnerability Management Support	dhsinfosechelpdesk@HQ.DHS.GOV
FAQ	Q: Why are assets that have no vulnerabilities scored as 0%? A: Servers, Workstations, and Laptops are required to be credentialed scanned. If the credentialed flag is not present, these assets will fail the metric. Q: Can the credentialed flag be overwritten? A: No. Once the credentialed flag is set for an asset, it remains for the reporting cycle, regardless of any new scans that are imported. Q: Why am I getting penalized for vulnerabilities that cannot be patched? A: These metric scores vulnerabilities, not patch-ability. If an asset reports a vulnerability, it will be scored.

A.9 Configuration Management-HVA

Detail	Description
Metric	Configuration Management-HVA
Metric Type	Implementation
Purpose	This metric will ensure that Components are applying configuration baselines and monitoring their assets.
Data Source	CDM/Splunk
Reporting Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams

Special Conditions	Checking PASS/FAIL. Asset Configuration Scores are based on the percentage of SCAP checks passed. All applicable OS are evaluated using CAT I, CAT II and CAT III STIG checks. To receive credit, Components must submit the specific SV (Rule ID) or WN (STIG ID) for each check that was performed, and the result of each test. If Expected Checks are not present, missing checks will count as FAILED checks. Checks that return "error" or "warning" will not count as failed. OS determines Applicability to this metric. However, assets with certain device roles of "are not evaluated." Please reference Universal Device Role List and the table of Available Configuration Audit Files for more information. Note: This list will be updated periodically throughout the year. For the most current list, please visit https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx
Description	% of applicable HVA assets meeting and passing required configuration checks.
Target	90%
Metric Calculation	Asset Configuration Score: # of expected checks passed/ # of expected checks. Weighted CAT I=50%, CAT II=30%, CAT III=20% System Configuration and Component Scores are a roll up from the Asset scores.
Splunk Reports	CSM and CSM_Details
Configuration Management Support	dhsinfosechelpdesk@HQ.DHS.GOV
FAQ	Q: Why are my assets failing? A: They are not passing enough of the expected checks. Q: Why are my assets not returning enough checks? A: This is likely because an incorrect or misconfigured audit file is being used. Please refer to

Detail	Description
	https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx for the latest audit files. Q: How can I find the list of applicable OS and the expected number of checks? A: Please refer to https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx for the latest Configuration Applicable OS and expected checks. Q: How does CISOD determine what OS is Applicable? A: Only OS that have DHS provided audit files are applicable. All audit files are available on DHS Connect http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx Q: How does CISOD determine the expected # of checks? A: CISOD tests the audit scripts and records the number of checks returned prior to the file being made available on DHS Connect.

A.10 Configuration Management-Other

Detail	Description
Metric	Configuration Management-Other
Metric Type	Implementation
Purpose	This metric will ensure that Components are applying configuration baselines and monitoring their assets.
Data Source	CDM/Splunk
Reporting Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams

Special Conditions	Checking PASS/FAIL. Asset Configuration Scores are based on the percentage of SCAP checks passed. All applicable OS, including Windows 10, are evaluated using CAT I, CAT II and CAT III checks. To receive credit, Components must submit the specific SV (Rule ID) or WN (STIG ID) for each check that was performed, and the result of each test. If Expected Checks are not present, missing checks will count as FAILED checks. Checks that return "error" or "warning" will not count as failed. OS determines Applicability to this metric. However, assets with certain device roles of "are not evaluated." Please reference Universal Device Role List and the table of Available Configuration Audit Files for more information. Note: This list will be updated periodically through the year. For the most current list, please visit https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx
Description	% of applicable non-HVA assets meeting and passing required configuration checks.
Target	90%
Metric Calculation	Asset Configuration Score: # of expected checks passed/ # of expected checks. Weighted CAT I=50%, CAT II=30%, CAT III=20% System Configuration and Component Scores are a roll up from the Asset scores.

Detail	Description
Configuration Management Support	dhsinfosechelpdesk@HQ.DHS.GOV
FAQ	Q: Why are my assets failing? A: They are not passing enough of the expected checks. Q: Why are my assets not returning enough checks? A: This is likely because an incorrect or misconfigured audit file is being used. Please refer to http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx for the latest audit files. Q: How can I find the list of applicable OS and the expected number of checks? A: Please refer to https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx for the latest Configuration Applicable OS and expected checks. Q: How does CISOD determine what OS is Applicable? A: Only OS that have DHS provided audit files are applicable. All audit files are available on DHS Connect http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx Q: How does CISOD determine the expected # of checks? A: CISOD tests the audit scripts and records the number of checks returned prior to the file being made available on DHS Connect.

A.11 Host Based Defense

Detail	Description
Metric	Host Based Defense
Metric Type	Effectiveness
Purpose	To ensure that anti-virus is installed and current, and HIPS are installed and enabled on all endpoint devices.
Data Source	CDM/Splunk
Reporting Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	In FY23 DHS Scorecard for Host Based Defense will start to use the CDM Elastic Dashboard data for those Components using CrowdStrike and for those that don't manual submission will continue. Determining malware defense applicability • The device role is used to determine malware defense applicability

	• Two flags are associated with each device role
	  o Endpoint Applicable to measure antivirus age HIPS Applicable to check if intrusion prevention is enabled
	Determining malware defense pass/fail
	• Age of antivirus is calculated by subtracting the Antivirus Date from the Last Scan Date.
	• The Last Scan Date is modified by any file, including Nessus, Symantec, and McAfee
	• If age of antivirus is less than or equal to 15 days, then the antivirus portion of malware defense passes.
	• If HIPS is found to be enabled, then the HIPS portion of malware defense passes.
	• Any one of the following values is accepted as HIPS enabled:
	  o Enabled
	  o Green
	  o Host IPS Enabled
	  o On
	  o Online
	  o True
	  o Yes

Description	% of assets meeting endpoint security requirements such that anti-virus is installed and current and Host Intrusion Protection (HIPS) is installed and enabled. Anti-Virus must have been updated within 15 days from the scan date for every endpoint. The score was weighted equally, 50% for Anti-virus and 50% for HIPS.
Target	95%
Metric Calculation	(0.5 x number of applicable endpoints with updated Anti-virus / number of applicable endpoints) + (.05 x number of applicable endpoints with HIPS enabled / number of applicable endpoints)
Splunk Reports	HostBasedDefense
Malware Defense Support	dhshqcontinuousmonitoring@hq.dhs.gov
FAQ	Q: I have HIPs on my asset, but it is still failing, why? A: The HIPs value must be flagged in the correct column and provide one of the following values: Enabled, Green, Host IPS Enabled, On, Online, True, Yes, or 1.

A.12 Indicators of Compromise Receiving Metric

Detail	Description
Metric	Indicators of Compromise Receiving
Metric Type	Operational
Purpose	This metric ensures that Components are receiving Classified and Unclassified IOCs, can determine if the IOC is impacting their environment and are able to perform an enterprise search for the IOC. This metric supports establishing and maintaining baseline cyber health for DHS.
Data Source	DHS Network Operations Security Center (NOSC)
Reporting Frequency	Monthly
Responsible Parties	Security Director, NOSC Branch Chief, Government Watch Officer, NOSC Monitoring and Analysis Teams, Incident Response Teams.
Special Conditions	Capabilities include where in the IDC the event occurred, infection source, time to implement countermeasures, place in the IDC where countermeasures are implemented, and time to report to NOSC.
Description	% of capability to receive an IOC and perform enterprise-wide sweeps for them. Note: Capabilities include classified access, time to acknowledge, time for search and determination of impact, and time to report to NOSC.
Target	100%
Metric Calculation	3 Phases: Phase 1: Acknowledgement on C-LAN • Full Credit (100%) for acknowledging within 24 hours of original notification • Partial Credit (50%) for acknowledging after 24 hours • No Credit (0%) if no acknowledgement Phase 2: Acknowledgement on A-LAN • Full Credit (100%) for acknowledging within 24 hours of original notification • Partial Credit (50%) for acknowledging after 24 hours • No Credit (0%) if no acknowledgement Phase 3: Reporting Host Sweep results using the IOC Tracker • Full Credit (100%) for completion within 48 hours of original notification • Partial Credit (50%) for completion after 48 hours • No Credit (0%) for providing no results Points are awarded for each phase; Green =100, Yellow = 50, Red = 0.

Detail	Description
	Total of 3 Phases/300*100=Final Score %
Crystal Reports	FY23 Daily Scorecard
Indicators of Compromise Support	dhsinfosechelpdesk@HQ.DHS.GOV
FAQ	Q: Where does this data come from? A: The data comes to CISOD in a report from NOSC. Q: Can I get a copy of this report? A: CISOD can provide Compliance Designees with Component- specific data from the NOSC report. Please send request to dhsinfosechelpdesk@HQ.DHS.GOV

A.13 Social Engineering

Detail	Description
Metric #1	Did Components conduct quarterly phishing exercises to assess the effectiveness of their training?
Metric Type	Execution (Yes or No)
Purpose	This metric determines whether a Component met the requirement to conduct quarterly phishing exercises.
Data Source	Data Call spreadsheet, self-reporting from the DHS CISOD Policy Team using the Risk Report Template Excel file.
Reporting Frequency	Quarterly
Responsible Parties	Components
Special Conditions	None
Description	Phishing exercises help to assess the effectiveness of a component's training program.
Target	Pass/Fail
Detail	**Description**
Metric #2	Components must test 100% of their userbase on a quarterly basis.
Metric Type	Execution (Yes or No)
Purpose	This metric is to determine if Components tested 100% of their userbase on a quarterly basis.
Data Source	Data Call spreadsheet, self-reporting from the DHS CISOD Policy Team using the Risk Report Template Excel file.
Reporting Frequency	Quarterly

Responsible Parties	Components
Special Conditions	None
Description	Provides an acceptable sampling of users across the Enterprise.
Target	100% = GREEN 50% - 99% = YELLOW 0 - 49% = RED

Detail	Description
Metric #3	Social Engineering – Click Rate
Metric Type	Effectiveness (Click Rate)
Purpose	Based on the "Complexity - Thresholds of Success", the percentage of recipients who click on a phishing link inside the email will help determine if training is successful and effective.
Data Source	Data Call spreadsheet, self-reporting from the DHS CISOD Policy Team using the Risk Report Template Excel file.
Reporting Frequency	Quarterly
Responsible Parties	Components
Special Conditions	Changes per quarter – see "Complexity - Thresholds of Success" **Metric for red/yellow/green changes by quarter based on expected level of complexity.
Description	Evaluates user's cybersecurity awareness skills and measures their progress.
Target	See "Thresholds of Success"

Detail	Description
Metric #4	Social Engineering – Complexity
Metric Type	Complexity
Purpose	Link to NIST Phish Scale https://resources.infosecinstitute.com/topic/the-phish-scale-how-nist-is-quantifying-employee-phishing-risk/
Data Source	Data Call spreadsheet, self-reporting from the DHS CISOD Policy Team using the Risk Report Template Excel file.
Reporting Frequency	Quarterly
Responsible Parties	Components
Special Conditions	Metric for red/yellow/green changes by quarter based on expected level of complexity.
~~Description~~	~~Evaluates user's cybersecurity awareness skills and measures their progress.~~

Target	See "Thresholds of Success"

Complexity – Thresholds of Success

Metrics 3 and 4 are broken down into the following and are based on the NIST Phish Scale:

Quarter 1	Quarter 2	Quarter 3	Quarter 4
Complexity: MODERATE	Complexity: MODERATE	Complexity: HIGH	Complexity: HIGH
CLICK RATE OF: 25% or less = GREEN 26%-35% = YELLOW >35% = RED	CLICK RATE OF: 25% or less = GREEN 26%-35% = YELLOW >35% = RED	CLICK RATE OF: 35% or less = GREEN 36%-50% = YELLOW >50% = RED	CLICK RATE OF: 35% or less = GREEN 36%-50% = YELLOW >50% = RED

APPENDIX B: SUPPLEMENTAL MONTHLY FISMA SCORECARD METRICS

PAGE 2-Supplemental	FY23 Updates/Descriptions
High Value Asset Systems	# of SBU reportable systems in CISOD inventory listed as a High Value Asset.
Other Reportable Systems	# of SBU reportable systems in CISOD inventory listed as something other than HVA.
Scanned Assets	# of assets reported in Component scans submitted to CISOD within the current reporting month, including assets not assigned to a FISMA system
Known Assets Reported (from ServiceNow)	Represents total assets reported on FISMA Data Call form.
Prohibited OS	# of assets detected running operating systems that are either not listed OR listed as Prohibited on the TRM
Cyber Hygiene (Critical/High/Moderate)	# of critical, high, and moderate vulnerabilities affecting public-facing websites and services reported in the last Cyber Hygiene report of each month.
Systems Passing Privacy Checks	Additional detail to help explain Security Authorization scores, this metric will indicate the % of systems that are failing Security Authorization solely due to Privacy Checks. 100% = Green; 99-95% = Yellow; <95= Red
POAMS expiring in 30|60|90 days	POAMS expiring in 30|60|90 days is when they will begin to fail.
Data Exfiltration (Reflects CIO Metric 3.8)	DHS inspects all traffic traversing the TIC for unencrypted data, along with header information for encrypted data.
HVA Systems without Alternate Sites (NOSC)	Based on CIO FISMA Reporting Data, reports the number of High Availability HVA systems that do not have an alternate processing site identified and provisioned.
HVA Systems without Network Segmentation (ServiceNow)	Based on CIO FISMA Reporting Data call, reports the number of HVA systems' network not segmented from other accessible systems and applications in the agency's network(s).

MFA and Encryption (2.1)	Quarterly data call
Critical Software (4.0)	Quarterly data call
Social Engineering – Was a Quarterly Phishing Exercise Conducted?	Did Components conduct quarterly phishing exercises to assess the effectiveness of their training?
Social Engineering - % of Population Tested	Components must test 100% of their userbase on a quarterly basis. **Red/0-49% Yellow/ 50-99% Green /100%**
Social Engineering – Click Rate	Based on the "Thresholds of Success"
Social Engineering - Complexity	Reflects the complexity of the exercise conducted. Q1/Q2=Moderate Q3/Q4=High.

PAGE 3-Supplemental	Description
Number of GFE mobile devices.	Number of GFE mobile devices.
Number of BYOD mobile devices.	Number of BYOD mobile devices.
Number of GFE mobile devices operating under enterprise-level mobile device management that includes, at a minimum, agency defined user authentication requirements on mobile devices and the ability to remotely wipe and/or remove agency data from the devices.	Number of GFE mobile devices operating under enterprise-level mobile device management that includes, at a minimum, agency defined user authentication requirements on mobile devices and the ability to remotely wipe and/or remove agency data from the devices.
BYOD same as above	BYOD same as above
Number of managed GFE mobile devices where users are unable to remove their mobile device management (MDM) or enterprise mobility management (EMM) profile without administrator approval. (NIST 800-53r4 CM-5)	Number of managed GFE mobile devices where users are unable to remove their mobile device management (MDM) or enterprise mobility management (EMM) profile without administrator approval. (NIST 800-53r4 CM-5)
BYOD same as above	BYOD same as above
Number of managed GFE mobile devices the agency enforces the capability to	Number of managed GFE mobile devices the agency enforces the capability to deny access to agency enterprise services (through the MDM or EMM policy) when security and operating system updates

deny access to agency enterprise services (through the MDM or EMM policy) when security and operating system updates have not been applied within a given period of time based on agency policy or guidance.	have not been applied within a given period of time based on agency policy or guidance.
BYOD same as above	BYOD same as above
Number of managed GFE mobile devices from where the agency enforces the capability to prevent the execution of unauthorized software (e.g., deny list, approve list, or cryptographic containerization) through the MDM or EMM. (NIST 800-53r4 CM-7)	Number of managed GFE mobile devices from where the agency enforces the capability to prevent the execution of unauthorized software (e.g., deny list, approve list, or cryptographic containerization) through the MDM or EMM. (NIST 800-53r4 CM-7)
BYOD same as above	BYOD same as above
Number of managed GFE mobile devices that require derived PIV credentials for mobile device transactions (e.g., authentication, secure email). (NIST SP 800-63-3) (OMB M-19-17)	Number of managed GFE mobile devices that require derived PIV credentials for mobile device transactions (e.g., authentication, secure email). (NIST SP 800-63-3) (OMB M-19-17)
BYOD same as above	BYOD same as above
What percent of your GFE mobile devices are covered by a mobile threat defense (MTD) solution? (NIST SP 800-124 Rev.2)	What percent of your GFE mobile devices are covered by a mobile threat defense (MTD) solution? (NIST SP 800-124 Rev.2)
What percent of your BYOD mobile devices are covered by a mobile threat defense (MTD) solution? (NIST SP 800-124 Rev.2)	What percent of your BYOD mobile devices are covered by a mobile threat defense (MTD) solution? (NIST SP 800-124 Rev.2)

APPENDIX C: POA&M CHECKLIST

Quality Checks	Requirement
Milestone Check	POA&M must have at least 2 milestones or it will fail on the scorecard.
Open Check	Program POA&MS- POAM must be open less than five years from Creation Date OR have a Policy Waiver AND waiver expiration date not reached. System POA&MS- • POAM must be open less than one year from Creation Date OR have a Policy Waiver AND waiver expiration date not reached
Criticality Check	POA&Ms must have Severity Level of High, Moderate, or Low selected.
Identified Check	Item Identified During field cannot be "Null"
POC Check	POA&M includes POC name and Phone or Email.
Scheduled Completion Check	Program POA&Ms Scheduled completion date is not 'null' AND Number of days between creation date and scheduled completion date must be less than or equal to (5 years) System POA&MS: • Scheduled completion date is not 'null' AND Number of days between creation date and scheduled completion date must be less than or equal to 365 days (1 year)
POA&MS with Status of Not Started are only scored on the Status Check	POA&M Workflow Status cannot be 'POAM Auto Approved' if POAM Status is 'Not Started'
Artifact(s)	An appropriate artifact should be uploaded as an attachment to the POA&M to support closure for audit validations. The artifact can be a document produced as a result of the remediation process, such as a Contingency Plan Test report, a screenshot showing the correct setting for a control, or a memo that describes the action taken or refers to other documentation.

APPENDIX D: POA&M WAIVERS

If a system cannot meet the minimum set of security controls required by DHS Sensitive Systems Policy Directive 4300A, a waiver must be approved by the component AO or delegate CISO and submitted to DHS CISOD. The waiver duration is set by the Component CIO. The waiver policy is provided in Section 1.5 of DHS Sensitive Systems Policy Directive 4300A, and the process to request a waiver is documented in the *DHS 4300A Sensitive Systems Handbook*, Attachment B, "Waiver Request Form." Note that approval of a waiver is not guaranteed.

Signed waivers must be uploaded into CSAM as documentation before changing a POA&M status to "Waiver." Waivers are tracked by the DHS CISO Policy Team and the DHS CISOD POA&M Team via the CISO Reporting Tool. For Weakness Remediation scoring, POA&Ms with the status of "Waiver" are cross-checked by the ISO Reporting Team with data provided by the Policy Team. It is the responsibility of the Policy Team to notify the reporting team of all approved POA&M waivers.

POA&Ms that fail the cross-check will fail the POA&M Status Check as outlined in Appendix C of this document. The status of waivers can be monitored via the Weakness Remediation report in Crystal Reports.

APPENDIX E: POA&M REASONABLENESS CRITERIA

The POA&M reasonableness criteria were created to address an OIG FISMA recommendation that DHS ensure POA&Ms are authorized to enact and deter the use of placeholder data such as $1 or $0. The criteria are included with Metric 5: Weakness Remediation.

The POA&M reasonableness criteria does not replace the remediation planning process, as described in Attachment H to the *DHS 4300A Sensitive Systems Handbook, "*DHS POA&M Process Guide." The resource estimates were developed to address a range of data that constitutes the minimum resources "reasonable" for developing POA&Ms. They are not intended as, and should not be used as, a guideline for the cost to correct a weakness.

The Reasonable Resource Matrix for NIST 800-53 controls provides an estimate of the minimum resources required to remediate each NIST 800-53 control weakness. It is based on a nominal labor rate of $100 per hour and does not include other direct expenses such as those for hardware or software). Because of the wide range of potential circumstances affecting any specific control, the "best case" was used to determine Level of Effort (LOE).

General guidelines for resource estimates:
Documents, such as a Component or system level auditing policy (e.g., policies, procedures, etc.) require a minimum of four hours or $400 to complete, while configuration-hardening weaknesses require a minimum of 30 minutes or $50. In some cases, only one part of a control may need remediation. The best case could require a system administrator to close a single port, or configure a setting on a server, necessitating only a minimal amount of time. Resources needed to prepare the Authorization document are based on estimated times. For IT security controls where a cost cannot be estimated due to the complexity or unknown factors (e.g., installing a fire suppression system), a nominal $50 cost is consistently listed.

APPENDIX F: UNIVERSAL DEVICE ROLE LIST

If a new device roll is needed, please contact ISO.Reporting@hq.dhs.gov

Device Role	Device Class	Endpoint Applicable	Software Applicable
Appliance	Other	FALSE	FALSE
Appliance - monitor fueling pump/data monitor	Other	TRUE	FALSE
Application	Other	FALSE	FALSE
Array	Other	FALSE	FALSE

Badge/card reader	Other	FALSE	FALSE
Blade Server	Other	FALSE	FALSE
Camera	Other	FALSE	FALSE
Cisco Switch	Other	FALSE	FALSE
Controller	Other	FALSE	FALSE
Controller/Server	Other	FALSE	FALSE
DMZ L3 Switch	Other	FALSE	FALSE
DVR	Other	FALSE	FALSE
ESX VMWare Server	Other	FALSE	FALSE
Firewall	Other	FALSE	FALSE
Generic Linux	Other	FALSE	FALSE
Handheld	Other	FALSE	FALSE
Hardware	Other	FALSE	FALSE
Hardware/Appliance	Other	FALSE	FALSE
Hyperconverged Appliance	Other	FALSE	FALSE
Infoblox	Other	FALSE	FALSE
Interface Panel	Other	FALSE	FALSE
KVM	Other	FALSE	FALSE
Laptop	Laptop	TRUE	TRUE
Laptop (Windows)	Laptop	TRUE	TRUE
Linux Device	Other	FALSE	FALSE
Load Balancer	Other	FALSE	FALSE
Mainframe	Server	FALSE	TRUE
Management Interface	Other	FALSE	FALSE
NAM Traffic Analyzer	Other	FALSE	FALSE
Network Optimization	Other	FALSE	FALSE
Network Switch	Other	FALSE	FALSE
NPVW	Workstation	TRUE	TRUE
PBX	Other	FALSE	FALSE
Power Device	Other	FALSE	FALSE
Printer	Other	FALSE	FALSE
RFID scanner	Other	FALSE	FALSE

Riverbed	Other	FALSE	FALSE
Router	Other	FALSE	FALSE
SAN	Other	FALSE	FALSE
Sensor	Other	FALSE	FALSE
Server	Server	TRUE	TRUE
Server (Non-Windows)	Server	TRUE	TRUE
Server (Windows)	Server	TRUE	TRUE
Server/AIX	Server	TRUE	TRUE
Server/EPO	Server	TRUE	TRUE
Server/Linux	Server	TRUE	TRUE
Server/Solaris	Server	TRUE	TRUE
Server/Sophos	Server	TRUE	TRUE
Server/Symantec	Server	TRUE	TRUE
Storage	Other	FALSE	FALSE
Switch	Other	FALSE	FALSE
Tablet	Other	FALSE	FALSE
Tape Backup	Other	FALSE	FALSE
Thin Client	Other	FALSE	FALSE
UNKNOWN	Other	FALSE	FALSE
UPS	Other	FALSE	FALSE
Video	Other	FALSE	FALSE
Virtualization Platform	Other	FALSE	FALSE
VMWare	Other	FALSE	FALSE
VoIP	Other	FALSE	FALSE
Wireless Access Point	Other	FALSE	FALSE
Workstation	Workstation	TRUE	TRUE
Workstation (Non-Windows)	Workstation	TRUE	TRUE
Workstation (Windows)	Workstation	TRUE	TRUE

APPENDIX G: RESOURCES, REFERENCES, AND SITE LINKS

Title	Site Link
CMWG SharePoint Site	https://mgmt-ocio-sp.dhs.gov/ciso/cmwg/default.aspx
Configuration Baseline Audit Files	https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx
Configuration Management Guidance	https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx
Configuration Standards for Information Systems – Interim Policy Memorandum	https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/Memo_Configuration_Standards.pdf
Crystal Reports	https://dhscrystal.dhs.gov/BOE/BI/
DHS Connect CISO Website	https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/Default.aspx
DHS Executive FISMA Scorecard Page	https://mgmt-ocio-sp.dhs.gov/ciso/CRMC/FSMBranch/DHSSupport/FISMAScorecard/SitePages/Home.aspx?RootFolder=%2Fciso%2FCRMC%2FFSMBranch%2FDHSSupport%2FFISMAScorecard%2FShared%20Documents%2FFY20%20Scorecards&FolderCTID=0x01200068A760EDFE93AB43A2E346A260498DDE&View=%7BBDB4131C%2DA3C6%2D475A%2D989F%2D7F098B0094D9%7 D
DHS FISMA Inventory Methodology	https://mgmt-ocio-sp.dhs.gov/ciso/im/Pages/inventmgmt.aspx
FY22 CIO Annual FISMA Metrics	Chief Information Security Officer (dhs.gov)
Inventory Management SharePoint Site	https://mgmt-ocio-sp.dhs.gov/ciso/im/Pages/inventmgmt.aspx
ISO Reporting	ISO.Reporting@hq.dhs.gov
OMB Max Portal	https://max.gov/maxportal/home.action
OMB Memorandum M-14-03	https://mgmt-ocio-sp.dhs.gov/ciso/fisma%20reporting/Shared%20Documents/FY14%20FISMA%20Guidance/m-14-03.pdf
Ongoing Authorization SharePoint Site	https://mgmt-ocio-sp.dhs.gov/ciso/compliance/Information%20Assurance/Forms/AllItems.aspx?RootFolder=%2Fciso%2Fcompliance%2FInformation%20Assurance%2FOngoing%20Authorization&FolderCTID=0x01200059821680FD99394DBF0EBB3AE264058D&View=%7B4C6EEEBC%2D532D%2D4511%2D9376%2DDDD337CA1B1F%7D
ServiceNow	DHS CISOD Homepage - CISOD Service Portal

	(servicenowservices.com)
Windows 10 Secure Host Baseline Implementation	https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/Memo_Windows10.pdf
EO 14028	Executive Order on Improving the Nation's Cybersecurity | The White House
DHS 4300A	DHS 4300A Sensitive Systems Handbook | Homeland Security

APPENDIX H: CYBERSECURITY CDM VULNERABILITY PATCH STATUS

Cybersecurity CDM Vulnerability Patch Status

Percent of DHS endpoints identified with Critical and High vulnerabilities patched within 30 days.

The Metrics & Reporting team used the component scan data submitted through CDM to estimate ability to patch endpoints monthly.

Challenges:

- We do not see patching data, but rather the result of patching (i.e., CVEs from previous scans are no longer seen in new scans).
- Components can submit scans throughout the month, we do not have a true "30 day" window, but rather a month-to-month window.

Activities:

Because our calculation is based on CVEs, the following adjustments were made:

1. Excluded are CVEs no longer found in NIST National Vulnerability Database (NVD).

Excluded are CVEs with a CVSS < 7.0 as the focus is on Critical & High CVEs.

Excluded are CVEs found in current month but not in previous month, which would not be 30 days old.

Excluded are assets not found in both the previous month and current month.

Asset level calculation

- The CVEs are counted that are found in the previous month (TotPrevCVE).
- The CVEs are counted that were in the previous month but are not present in the current month (TotCurCVE); these are assumed to be patched.
- Asset Patch Percent = TotCurCVE / TotPrevCVE * 100.0 (If TotPrevCVE = 0 then Asset Patch Percent is zero).

Component level calculation

- Count all assets with a Patch Percent greater than zero (TotalAssets).
- Sum all asset patch percentages (PatchPctSum, only assets with Asset Patch Percent greater than zero).

- Component Patch Percent = PatchPctSum / TotalAssets
- Current logic sets Component Patch Percent to zero if Total Assets with CVEs are 0 so 100% is assumed.

Achievement:

Through this process, it is possible to calculate how many endpoints had remediated critical and high CVEs between monthly reporting cycles.

APPENDIX I: ITEMS IN ISPP THAT FISMA QUARTERLY REPORTING AND THE MONTHLY SCORECARD HAVE IN COMMON THAT SUPPORTS OMB FISMA METRICS

Page 1 of Scorecard:

- Security Authorization – HVAs & Other scorecard metric for this is different because it takes other things into account, but this is most closely tied in with metrics 1.1.1, 1.1.2, 1.1.3, and 1.1.4 on the FISMA Quarterly reporting and on page 16 of the ISPP.
- Scan compliance - we have a metric that is systems scanned via SCAP. Not sure if this is the same thing. This is metric 2.1 (number scanned) divided by total number of endpoints for the FISMA Quarterly reporting and on page 21 of the ISPP.
- Hardware Asset Management – Metric 3.9 for FISMA reporting on the FISMA Quarterly reporting and on page 21 of the ISPP.
- Software Asset Management – Metric 3.10. (Unauthorized software detection) divided by metric 1.2.1 (1.2.1 is all endpoints) on the FISMA Quarterly reporting and on page 33 of the ISPP.

Supplemental Pages:

- Number of mobile devices
- Number of mobile devices operating under enterprise-level mobile device management that includes, at a minimum, agency defined user authentication requirements on mobile devices and the ability to remotely wipe and/or remove agency data from the devices
- Number of managed mobile devices from 1.3.3. (GFE) or 1.3.4. (BYOD) where users are unable to remove their mobile device management (MDM) or enterprise mobility management (EMM) profile without administrator approval. (NIST 800-53r4 CM-5)
- Number of managed mobile devices from 1.3.3. (GFE) or 1.3.4. (BYOD) where the agency enforces the capability to deny access to agency enterprise services (through the MDM or EMM policy) when security and operating system updates have not been applied within a given period of time based on agency policy or guidance
- Number of managed mobile devices from 1.3.3. (GFE) or 1.3.4. (BYOD) where the agency enforces the capability to prevent the execution of unauthorized software (e.g., deny list, approve list, or cryptographic containerization) through the MDM or EMM. (NIST 800-53r4 CM-7)
- Number of managed mobile devices from 1.3.3. (GFE) or 1.3.4. (BYOD) that require derived PIV credentials for mobile device transactions (e.g., authentication, secure email). (NIST SP 800-63-3) (OMB M-19-17)

- What percent of your mobile devices (GFE and BYOD) are covered by a mobile threat defense (MTD) solution? (NIST SP 800-124 Rev.2)

APPENDIX J: SECURITY AUTHORIZATION CRYSTAL REPORT MATRIX

SA Report Crystal	Data type	Description	Impact	Requirements	Data Source	Write Permissions
Component	varchar	Component responsible for the system	Used to determine which Component the system score rolls up to for the DHS Month Scorecard		System Information --> System Identification --> Identification --->Component	Dept, Comp. Lead, ISSM and ISSO
System Name	varchar	System Name	Used to identify individual systems for the purpose of reporting and scoring.		System Information --> System Identification --> Identification --> External ID	Dept
FISMAID	varchar	FISMAID	Used to identify individual systems for the purpose of reporting and scoring.		System Information --> System Identification --> Identification --> System Name	Dept, Comp. Lead, ISSM and ISSO
HVA	True/False	Is system an HVA?	Security Authorization is split between HVA and Non-HVA systems. This flag is used to ensure the correct systems are scored for each metric	TRUE IF *Agency Defined Data Items- High Value Asset = Yes*	System Information --> System Identification --> Agency Defined Data Items --> High Value Asset	Dept
CFO	True/False	Is system CFO designated?	Informational	TRUE IF Agency Defined Data Items- CFO Designation = Yes	System Information --> System Identification --> Agency Defined Data Items -->CFO Designation	Dept, Comp. Lead, ISSM and ISSO
Auth Type	ATO/OATO /ATP	Shows if the system has a regular ATO is in Ongoing Authorization (OATO) or has an Authority to Proceed (ATP)	Used to determine which checks are applicable to the system. ATO and OATO system must pass all 5 checks. ATP system only need to pass the Authorization Status Check		System Overview --> Security Authorization -->Authorization Status	DHS DR Team
Security Authorization on Status	Pass/ Fail	Indicates if the system is passing the DHS Monthly Scorecard metric for Security Authorization	Fail indicated one or more required checks are not being met.	Systems with ATO or OATO must pass all 5 Security Authorization checks: Auth Status Check, DR Check, CP Check, CPT Check, and Privacy Check. ATP systems must only pass the Auth Status check.	DIAR2	

Auth Status Check	Pass/ Fail	Indicates if the system is passing the Authorization Status check	All systems must pass this check to pass the Security Authorization metric	Auth Date cannot be NULL and cannot be a future date If Expiration date < current date the system will fail the Auth Status check. If Expiration date = current date system will pass.	DIAR2	
DR Check	Pass/ Fail	Indicates if the system is passing the Document Review (DR) check	ATO and OATO systems must pass this check to pass the Security Authorization metric	Document Review Date cannot be NULL and cannot be a future date. Date indicates DHS DR Team has approved the systems Security Authorization package	DIAR2	
CP Check	Pass/ Fail	Indicates if the system has a valid Contingency Plan	ATO and OATO systems must pass this check to pass the Security Authorization metric	CP Date cannot be NULL and cannot be a future date	DIAR2	
CPT Check	Pass/ Fail	Indicates if the system has a valid Contingency Plan Test record	ATO and OATO systems must pass this check to pass the Security Authorization metric	CPT Date cannot be NULL, cannot be a future date, and must be within 1 year	DIAR2	
Privacy Check	Pass/ Fail	Indicated is the system has a valid PTA, PIA (if required) and SORN (if Required)	ATO and OATO systems must pass this check to pass the Security Authorization metric	PTA Date cannot be NULL, cannot be a future date, and must be within 3 years; IF PIA is Required PIA Date cannot be NULL, cannot be a future date, IF SORN is Required SORN date cannot be NULL, cannot be a future date	DIAR2	
Auth Date	mm/dd/yyyy	Reflects the Initial/ Most recent Authorization date	Used for the Auth Status Check	Date cannot be NULL and cannot be a future date	ATO/OATO: System Overview --> Security Authorization --> Last Authorization Date; ATP: Same or Status and Archive ATP Approval Date and Expiration date?	Dept
Auth Expiration	mm/dd/yyyy	Reflects when the current authorization will expire	Used for the Auth Status Check	If Expiration date < current date the system will fail the Auth Status check. If Expiration date = current date system will pass.	System Overview --> Security Authorization --> Expiration Date	Dept

Document Review Date	mm/dd/yyyy	Reflects date DHS DR team completed their review process and approved the system documentation.	Used for the DR Approval Check	Date cannot be NULL and cannot be a future date	System Overview --> Status & Archive --> Document Review Approval --> Date Completed	DHS DR Team
CPR Date	mm/dd/yyyy	Reflects the date the Contingency Plan review was completed by DHS Document Review Team	Used for the CP Check	Date cannot be NULL and cannot be a future date	System Overview --> Status & Archive --> Contingency Plan Review --> Date Completed	DHS DR Team *This date might not match the Contingency Plan (CP) Date Completed in the Continuity & Incident Response section under System Overview. This date is entered by the DHS DR Review Team on the Status and Archive page and reflect when they completed their review.
CPT Date	mm/dd/yyyy	Reflects the date of the most recent Contingency Plan Test	Used for the CPT Check	Date cannot be NULL, cannot be a future date, and must be within 1 year	System Overview --> Status & Archive --> Contingency Plan Test Review --> Date Completed	DHS DR Team *This date should match the actual Contingency Plan Test (CP) Test Date Completed in the Continuity & Incident Response section under System Overview but is entered by the DHS DR Review Team on the Status and Archive page after they have completed their review.
PTA Valid	True/False	Indicates if the PTA is meets requirements for Security Authorization	Used for the Privacy Check	TRUE IF Auth Status = ATO/ OATO AND PTA Date is not NULL, not a future date, and within 1 year	DIAR2	
PTA Date	mm/dd/yyyy	Reflects the date of the most recent Privacy Threshold Analysis	Used for the Privacy Check; Determines if the PTA is valid	Date cannot be NULL, cannot be a future date, and must be within 1 year of current date	System Overview --> Privacy --> Privacy Threshold Analysis --> Date Completed	DHS Privacy Team* *Currently field is open to all, but we are working towards limiting access
PIA Valid	True/False	Indicates if the PIA, if required, meets requirements for Security Authorization	Used for the Privacy Check	TRUE IF NOT REQUIRED OR REQUIRED AND PIA date is not NULL and not a future date	DIAR2	
PIA Required	True/False	Reflects if a PIA is "Required under E-Government Act"	Used for the Privacy Check; Determines if the PIA Date is required	TRUE IF *Privacy Impact Assessment Status* = "Required under E-Government Act"	System Overview --> Privacy --> Privacy Impact Assessment --> Status	DHS Privacy Team* *Currently field is open to all, but we are working towards limiting access

PIA Date	mm/dd/yyyy	Reflects the most recent PIA Completed date	Used for the Privacy Check; Used to determine if the PIA Date is valid	IF REQUIRED date cannot be NULL, cannot be a future date	System Overview --> Privacy --> Privacy Impact Assessment --> Date Completed	DHS Privacy Team* If DHS Privacy Team determines a new or updated PIA is required; this date will be removed by the DHS Privacy Team until the required action has been completed. This will cause the check to Privacy Check to fail. *Currently field is open to all, but we are working towards limiting access
SORN Valid	True/False	Indicates if the SORN, if required, meets requirements for Security Authorization	Used for the Privacy Check	TRUE IF NOT REQUIRED OR REQUIRED AND SORN date is not NULL and not a future date	DIAR2	
SORN Required	True/False	Indicates if a SORN is Required under Privacy Act	Used for the Privacy Check; Determines if the SORN Date is required	TRUE IF *System of Records Notice Status* = "Required under Privacy Act"	System Overview --> Privacy --> System of Records Notice --> Status	DHS Privacy Team* *Currently field is open to all, but we are working towards limiting access
SORN Date	mm/dd/yyyy	Reflects the SORN Published in Federal Register date	Used for the Privacy Check; Used to determine if the SORN is valid	IF REQUIRED date cannot be NULL, cannot be a future date	System Overview --> Privacy --> System of Records Notice List--> Published in Federal Register	DHS Privacy Team* *If DHS Privacy Team determines a new or updated SORN is required, this date will be removed by the DHS Privacy Team until the required action has been completed. This will cause the check to Privacy Check to fail. Currently field is open to all, but we are working towards limiting access

APPENDIX K. WEAKNESS REMEDIATION CRYSTAL REPORT MATRIX

WR Report Crystal	Data type	Description	Impact	Requirements	Data Source
Component	varchar	Component responsible for the system	Used to determine which Component the system score rolls up to for the DHS Month Scorecard		CSAM--> System Information --> System Identification --> Identification --> Component

System Name	varchar	System Name	Used to identify individual systems for the purpose of reporting and scoring.		CSAM--> System Information --> System Identification --> Identification --> External ID
FISMAID	varchar	FISMAID	Used to identify individual systems for the purpose of reporting and scoring.		CSAM--> System Information --> System Identification --> Identification --> System Name
WR Applicable	True/False	Indicates if the POA&M is impacting the overall Weakness Remediation score	If TRUE, POA&M is being scored against applicable quality and timeliness checks and impacting the Weakness Remediation metric	All OPEN POA&Ms and POA&MS COMPLETED within the current reporting month or previous two reporting months are applicable to scoring.	DIAR2
HVA	True/False	Is system an HVA?	If TRUE, POA&Ms for HVA systems weighted as 70% of the overall component	TRUE IF Agency Defined Data Items- High Value Asset = Yes	CSAM--> System Information --> System Identification --> Agency Defined Data Items -->
			score. If FALSE, POA&M weighted as 30% of the overall component score		High Value Asset
CFO	True/False	Is system CFO designated?	Informational		System Information --> System Identification --> Agency Defined Data Items --> CFO Designation

CSAM POA&M ID	varchar	Unique ID across all of CSAM	Informational		CSAM--> POA&M --> POA&M Listing--> POA&M ID
POA&M Number	varchar	POA&M Sequence number for individual systems	Informational		CSAM--> POA&M --> POA&M Listing--> POA&M Sequence
POA&M Passing	True/False	Indicates if the POA&M is passing the Weakness Remediation metric	if TRUE, POA&M has a positive impact on the system and component score. If FALSE POA&M is counting against the system and overall component score.	TRUE IF POA&M passes all required checks	DIAR2
POA&M Status Check	Pass/ Fail	Indicates if the POA&M is passing the Status Check	If FAIL, POA&M will count against the Weakness Remediation score	POA&M Workflow Status cannot be 'Draft - Created', 'Draft Approval Requested' or a succession of the two for longer than 30 days	DIAR2
POA&M Open	Pass/ Fail	Indicates if the	If FAIL, POA&M will	POA&M must be open less than	DIAR2

Check		POA&M is passing the Open check	count against the Weakness Remediation score	one year from Creation Date OR have a Policy Waiver AND waiver expiration date not reached	
Scheduled Completion Check	Pass/ Fail	Indicates if the POA&M is passing the Scheduled Completion check	If FAIL, POA&M will count against the Weakness Remediation score	Scheduled completion date is not 'null' AND Number of days between creation date and scheduled completion date must be less than or equal to 365 (1 year)	DIAR2
Criticality Check	Pass/ Fail	Indicates if the POA&M is passing the Criticality	If FAIL, POA&M will count against the Weakness Remediation	POA&Ms must have User Defined Criticality of High	DIAR2
Severity Level Check	Pass/ Fail	Indicates if the POA&M is passing the Severity	For Informational Purposes Only	POA&Ms must have Severity of Control Deficiency,	DIAR2
Control Link Check	Pass/ Fail	Indicates if the POA&M is passing the Control	Starting FY22 Q2 -If FAIL, POA&M will count against the Weakness Remediation score	POA&M must be tied to at least 1 control	DIAR2
Identified During Check	Pass/ Fail	Indicates if the POA&M is passing the Identified	If FAIL, POA&M will count against the Weakness Remediation	Item Identified During cannot be Null/Not Selected	DIAR2
Milestone Check	Pass/ Fail	Indicates if the POA&M is passing the Milestone check	If FAIL, POA&M will count against the Weakness Remediation score	Must have at least 2 milestones	DIAR2
POC Check	Pass/ Fail	Indicates if the	If FAIL, POA&M will	Assigned to' cannot be 'null'	DIAR2

		POA&M is passing the POC check	count against the Weakness Remediation score		
POA&M Status	Not Started Planned/Pending in Progress Delayed Cancelled Completed	Reflects one of the 6 POA&M status options in CSAM	Used to determine if the POA&M is applicable to Weakness Remediation scoring	POA&Ms with Status of Not Started, Planned/Pending, In Progress, or Delayed OR POA&Ms Completed in the current reporting month or previous 2 reporting months	CSAM--> POA&M --> POA&M Listing-- >POA&M Status
Workflow Status	Draft - Created Draft - Approval Requested POA&M Approved POA&M Approval Denied POA&M Auto Approved POA&M Cancellation Requested POA&M Close Requested Cancel Approved Cancel Denied Close Approved Close Denied Reopen POA&M	Reflects one of the 12 POA&M workflow status options in CSAM	Used to determine POA&M applicability to the Status Check	POA&MS with Status of Not Started are only scored on the Status Check	CSAM--> POA&M --> POA&M Listing-- >POA&M Workflow Status
Create Date	mm/dd/yyyy	Reflects the date the POA&M was created	Used to determine when the clock starts for the Open Check and Scheduled Completion Check	Cannot be Null; Cannot be a future date	CSAM--> POA&M --> POA&M Listing--> Create Date
Scheduled Completion Date	mm/dd/yyyy	Reflects the date component selects for the POA&M to be completed	Used to determine if the POA&M passes the Schedule Completion Date check	Scheduled completion date is not 'null' AND Number of days between creation date and scheduled completion date must be less than or equal to 365 days (1 year)	CSAM--> POA&M --> POA&M Listing--> Scheduled Completion Date

0

Actual Finish Date	mm/dd/yyyy	Reflects the actual date the POA&M is completed	Used to determine how long a completed POA&M will count towards the weakness remediation metric		CSAM--> POA&M --> POA&M Listing--> Actual Finish Date
Days Overdue	varchar	Reflects number of days, after 1 year, that a POA&M remains open without having a valid waiver in place	For Informational Purposes Only		DIAR2
Policy Waiver	True/False	Indicates if the POA&M has an approved policy waiver	If TRUE, POA&M will be scored as passing regardless of check results	Policy Waiver Approved must be TRUE AND Policy Waiver Expiration date must not have passed	CSAM--> POA&M --> POA&M Listing--> Policy Waiver Approved
Policy Waiver Expiration	mm/dd/yyyy	Reflects the date the POA&M policy waiver expires	Used to determine of the Policy Wavier is valid	Cannot be Null; Cannot be past date	CSAM--> POA&M --> POA&M Listing--> Policy Waiver Expiration
Criticality	Very Low Low Medium High Very High	Reflects the user identified criticality selected for the weakness	Used to determine if the POA&M passes the Criticality Check	POA&Ms must have criticality of Very High, High, medium, Low, or Very Low selected; Cannot be Null/	CSAM--> POA&M--> POA&M Listing--> User Identified Criticality
Severity	Control Deficiency Material Weakness Significant Deficiency Other Weakness NA		For Informational Purposes Only		CSAM--> POA&M --> POA&M Listing--> Severity

1

Controls	varchar	Reflects the specific controls that need to be addressed by the POA&M	Used to determine if the POA&M passes the Control Link Check, once implemented	POA&M must be tied to at least 1 control	CSAM--> POA&M --> POA&M Listing--> Controls
Item Identified During	Security Assessment Critical Control Review Vulnerability Assessment	Reflects where the item that triggered the POA&M was identified	Used to determine if the POA&M passes the Identified During Check	Item Identified During cannot be Null/Not Selected	CSAM--> POA&M --> POA&M Listing--> Item Identified During
Number of Milestones	varchar	Reflects the number of milestones associated with a particular POA&M	Used to determine if the POA&M passes the Milestone Check	Must have at least 2 milestones	CSAM--> POA&M --> POA&M Listing--> Number Milestones
Assigned To	varchar	Indicates the primary person responsible for work on the POA&M	Used to determine if the POA&M passes the POC Check	Cannot be Null	CSAM--> POA&M --> POA&M Listing--> Assigned To

APPENDIX L. Deprecated Protocols & Software

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 6, 2021

DECISION

MEMORANDUM FOR COMPONENTS CHIEF INFORMATION SECURITY OFFICERS

FROM: Kenneth Bible
Chief Information Security Officer

KENNETH W BIBLE
Digitally signed by KENNETH W BIBLE
Date: 2021.10.06 10:56:04 -04'00'

SUBJECT: **Development of a Deprecated Standard List**

Purpose: The purpose of this memorandum is to provide guidance on the development of Deprecated Standards List (DSL) for the Department.

Background: The DSL will provide DHS CISO and Component CISOs the opportunity to asses current protocols in use within their organizations and inform the enterprise on technologies which have been replaced by newer technologies. Discontinuing use of deprecated technologies in a timely, methodical manner is a basic security principle.

The CISO Council will review and approve the DSL on a semi-Annual basis, and the DSL (and future updates) will be transmitted to the DHS CIO for consideration at the CIO Council upon approval to inform their investment review decisions in guiding developers and purchasing agents.

The CISO Council will consider the level of threat, and risks to continued use of deprecated standards; however, for the purposes of managing the DSL, considerations of the level of difficulty involved in removal of the standard/technology from the enterprise should not be a deciding factor. The deprecated list must include standards that have been replaced. Standards that are still supported with patching and updates should not in general be included, since they may still be viable, and constitute a different requirement to be addressed in managing the technologies in the environment.

The DSL is not intended to be a prioritized list, since a number of factors play into the prioritization of removal of a standard from the enterprise; however, the CISO Council will designate a date for removal of each standard, after which a waiver must be submitted to the DHS CISO documenting the need for continued use. Removal date determination will be based on the following factors:

- Clear and active threat to the DHS enterprise
- "Blast radius" or scope of impact to compromises of the technology
- Current cyber threat intelligence

- State of exploitation and available mitigating strategies

The DSL will be developed by a consensus process in the CISO Council. Once consensus on inclusion of a standard has been reached, the removal date will be developed based on the factors above. Removal dates should be established that assertively drive the desired outline of removing the technology from the environment in a timely and methodical fashion.

Attachment: Table 1- Deprecated Standards List 1QFY22

Attachment: Table 1- DHS Deprecated Standards List Fiscal Year 2022

Protocol	Vulnerability	Background	Reference	Proposed Deprecation	Amplifying Instructions
NTLM	Vulnerability	There are several clear disadvantages to relying on NTLM authentication: Single authentication. NTLM is a single authentication method. It does not support multifactor authentication (MFA). The relatively simplistic form of password hashing makes NTLM systems vulnerable to several modes of attacks, including pass-the-hash and brute-force attacks. Outdated cryptography. NTLM does not leverage the latest advances in algorithmic thinking or encryption to make passwords more secure.	https://www.crowdstrike.com/cybersecurity-101/ntlm-windows-new-technology-lan-manager/ http://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/CISO%20ALL%20Documents/4300A%20SSPD%20v13.1.pdf 4300A Section 5.4.5.e	**Q2 FY22**	Beyond that date, systems still using NTLM on the DHS Enterprise will require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
FTP	Vulnerability	Clear text protocol. No security replaced by SFTP. Not blocked internally, may be allowed outbound on a case by case basis where security is not a concern. Possible to carve entire files from TCP stream and grab authentication (usernames and passwords).	https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final https://datatracker.ietf.org/doc/rfc8996/	**Q2 FY22**	Beyond that date, systems still using FTP on the DHS Enterprise will require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
TFTP	Vulnerability	TFTP "Trivial FTP" is occasionally used by NAs to flash network devices but that's point to point, direct cable connection. Need to ask the question from NAs to see how this is used.	https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r1.pdf	**Q2 FY22**	Beyond that date, systems still using TFTP on the DHS Enterprise will require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
TLS 1.0	Vulnerability	Vulnerable to MITM attack.	https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final https://datatracker.ietf.org/doc/rfc8996/	**Q2 FY22**	Beyond that date, systems still using TLS1.0 require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
TLS 1.1	Vulnerability	Vulnerable to MITM attack (POODLE). In 2018, FEMA did some clean up to remove outdated TSL protocols.	4300A Section 5.4.5.d	**Q2 FY22**	Beyond that date, systems still using TLS1.1 require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.

Protocol	Vulnerability Threat Risk	Background	Reference	Proposed Deprecation Date: By End of the Quarter Listed Below	Amplifying Instructions
Telnet	Vulnerability	Clear text protocol. Could be used but should be restricted if not tunneled or wrapped in secure TCP protocol such as SSH.	https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final https://datatracker.ietf.org/doc/rfc6176/	**Q2 FY22**	Beyond that date, systems still using Telnet require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
SMBv1/CIFS	Risk	Server Message Block (SMB) version 1 / Common Internet File Services (CIFS). Vulnerable to ransomware (wannacry, peytra), and other exploits: ETERNALBLUE, DOUBLE PULSAR, ETERNALROMANCE. Officially deprecated by Microsoft in 2014.	https://assets.extrahop.com/pdfs/security-advisories/insecure-protocols.pdf	**Q2 FY22**	Beyond that date, systems still using SMB/CIFS require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
SSL2	Threat	Basically Obsolete. Allows client and server to agree to less security. Uses MD5 hash algorithm for handshake authentication. MD5 is vulnerable to collision attacks. SSL2 largely outdated since 1996.	https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final https://datatracker.ietf.org/doc/rfc7568/ https://us-cert.cisa.gov/ncas/alerts/TA14-290A	**Q2 FY22**	Beyond that date, systems still using SSL2 require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
SSL3	Risk	Basically Obsolete. Uses MD5 hash algorithm for handshake authentication. MD5 is vulnerable to collision attacks. Largely outdated since 1999.	https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final https://datatracker.ietf.org/doc/rfc8429/	**Q2 FY22**	Beyond that date, systems still using SSL3 require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
3DES	Risk	Weak encryption. DES Banned in 2005 and 3DES replaced this algorithm by tripling the same weak method.	https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final https://datatracker.ietf.org/doc/rfc8429/	**Q3 FY22**	Beyond that date, systems still using 3DES require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
RC4	Threat	Not cryptographically secure. Does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.	https://assets.extrahop.com/pdfs/security-advisories/insecure-protocols.pdf	**Q3 FY22**	Beyond that date, systems still using RC4 require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.

Protocol	Vulnerability Threat Risk	Background	Reference	Proposed Deprecation Date: By End of the Quarter Listed Below	Amplifying Instructions
LLMNR	Vulnerability	Link-Local Multicast Name Resolution (LLMNR); Benefit: Identifying the host on the local subnet when DNS fails. Risk: MITM, Poisoning and SMB Relay. By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials.	https://datatracker.ietf.org/doc/draft-ietf-tls-md5-sha1-deprecate/ https://tools.ietf.org/id/draft-lvelvindron-tls-md5-sha1-deprecate-01.html	**Q3 FY22**	Beyond that date, systems still using LLMNR require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
MD5	Threat	Week algorithm due to high collisions in the resulting hash. Should be banded after 2023 according to NIST pub.	https://datatracker.ietf.org/doc/draft-ietf-tls-md5-sha1-deprecate/ https://tools.ietf.org/id/draft-lvelvindron-tls-md5-sha1-deprecate-01.html	**Q4 FY22**	Beyond that date, systems still using MD5 require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.
SHA-1	Risk	Not secure due to collision attack. It is possible for more than one files to have the same SHA-1 Hash. This makes it possible for the two different files to have the same signature allowing an attacker to deliver malicious content.	https://csrc.nist.gov/projects/hash-functions/nist-policy-on-hash-functions	**Q4 FY22**	Beyond that date, systems still using SHA-1 require a waiver from the DHS CISO. Waiver submissions must include a planned migration to a more secure protocol.

APPENDIX M: ACRONYMS AND ABBREVIATIONS

The following acronyms and abbreviations are used in this document:

Acronym	Definition
AO	Authorizing Official
ATO	Authority to Operate
ATP	Authority to Proceed

AV	Anti-virus
BYOD	Bring Your Own Device
CAP	Cross Agency Priority
CAT	Control Allocation Table
CCE	Common Configuration Enumeration
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMWG	Continuous Monitoring Working Group
CP	Contingency Plan
CPE	Common Platform Enumeration
CPT	Contingency Plan Test
CR	Change Request
CRMC	Cybersecurity Risk Management and Compliance
CSM	Configuration Settings Management
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
CVSS	Common Vulnerability Scoring System
CWG	Compliance Working Group
DIAR2	DHS Information Assurance Repository 2
DISA	Defense Information Systems Agency
DR	Document Review
EA	Enterprise Architecture
EIS	External Information System
ELA	Enterprise License Agreement
EOC	Enterprise Operations Center
ePO	McAfee ePolicy Orchestrator
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act

FOUO	For Official Use Only
FNR	Federal Network Resilience
FY	Fiscal Year
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GSS	General Support System
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
HVA	High Value Asset
HW	Hardware
HWAM	Hardware Asset Management
IA	Information Assurance
IACS	Information Assurance Compliance System
ICR	Inventory Change Request
ID	Identifier
IMT	Inventory Management Team
IOC	Indicators of Compromise
IP	Internet Protocol
IPT	Integrated Project Teams
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
LOE	Level of Effort
MAJ	Major Application
MES	Mission Essential System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAC	Network Access Control
NCATS	National Cybersecurity Assessment Technical Service

NIST	National Institute of Standards & Technology
NIST SP	NIST Special Publication
NOSC	Network Operations and Security Center
NSS	National Security System
NVD	National Vulnerability Database
OA	Ongoing Authorization
OCIO	Office of the Chief Information Officer
CISOD	Office of Chief Information Security Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OS	Operating System
PIA	Privacy Impact Assessment
PHI	Protected Health Information
PII	Personally Identifiable Information
PIV	Personal Identification Verification
POA&M	Plan Of Action & Milestone
PPWG	Performance Plan Working Group
PTA	Privacy Threshold Analysis
RMF	Risk Management Framework
SA	Security Authorization
SAR	Security Assessment Report
SBU	Sensitive But Unclassified
SCAP	Security Content Automation Protocol
SELC	Systems Engineering Life Cycle
SOC	Security Operations Center
SORN	System Of Records Notice
SP	Security Plan
SPII	Sensitive Personally Identifiable Information
SSI	Sensitive Security Information
SSP	System Security Plan
SAP	Security Assessment Plan

SW	Software
SWAM	Software Asset Management
TIC	Trusted Internet Connection
TRM	Technical Reference Model
URL	Uniform Resource Locator
VOIP	Voice over IP
VULN	Vulnerability Management