Homeland Security

OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

FY17 Information Security

DHS Information Security Performance Plan

Version 1.0

December 31, 2016

Protecting the Information that Secures the Homeland

Document Change History

Version	Date	Author	Description
1.0	Dec. 31, 2016	Teresa Proctor	Initial publication
1.0	Apr. 21, 2017	Genevieve Marquardt	Non-FOUO Version

CONTENTS

Executive Summary **1**

1. Introduction **3**
- 1.1 Purpose 3
- 1.2 Scope 3
- 1.3 Audience 4

2. Background **5**
- 2.1 Working Groups and Integrated Project Teams 5
- 2.2 Goals and Objectives 5
- 2.3 Strategy 6
- 2.4 Cybersecurity Maturity Model 7

3. FISMA Compliance Management **9**

4. Inventory Process **10**
- 4.1 System Inventory 10
  - 4.1.1 High Value Assets 10
  - 4.1.2 Mission Essential Systems 11
  - 4.1.3 Chief Financial Officer Designated Systems 11
- 4.2 Asset Inventory 12

5. Information Security Continuous Monitoring **14**
- 5.1 Existing ISCM Capability Groups and Tools 14
- 5.2 Continuous Diagnostics and Mitigation 15
- 5.3 ISCM Data 16
  - 5.3.1 Hardware and Software Asset Management 17
  - 5.3.2 Vulnerability Management 17
  - 5.3.3 Configuration Management 18
  - 5.3.4 Anti-Phishing/Malware 18
  - 5.3.5 Information Security Vulnerability Management 18
- 5.4 ISCM Data Collection, Aggregation, and Storage 19

6. Security Management Metrics **20**
- 6.1 Security Authorization 20
- 6.2 Common Controls 21
- 6.3 Ongoing Authorization 21
- 6.4 Document Review 24
  - 6.4.1 Document Review Methodology 25
  - 6.4.2 Initiation 26
  - 6.4.3 Package Categories 27
  - 6.4.4 Document Review Checklists 27
  - 6.4.5 Security Plan 28

6.5 Documenting Implemented Controls 29
6.6 Documenting Planned Controls 29
6.7 Documenting Control Inheritance 30
6.7.1 Contingency Plan and Contingency Plan Test 32
6.7.2 Security Assessment Plan 32
6.7.3 Security Assessment Report 33
6.7.4 Requirement Traceability Matrix 33
6.7.5 Review Results 33
6.7.6 Conference Calls 33
6.7.7 Re-Reviews 34
6.7.8 Component Auto-Validation 34
6.7.9 Privacy 34
6.7.10 Authorization Extensions 35
6.8 Weakness Remediation 35
6.9 Cyber Hygiene Scanning 36
6.10 CISO Security Reviews 36
6.10.1 Component Outreach Assist Visits 36
6.10.2 Critical Control Review 37

7. Enterprise and CIO FISMA Metrics 39
7.1 Information Security Continuous Monitoring 39
7.2 Anti-Phishing/Malware and Other Defenses 39
7.3 Mandatory PIV 41

8. CISO General Support 42
8.1 Outreach and Training 42
8.2 Security Training 42
8.2.1 Annual Information Technology Security Awareness 43
8.2.2 Privileged User Training 43

9. FISMA Reporting SharePoint 44
9.1 Component Forms/Data Submissions 44

10. DHS FISMA Scorecard and Reporting 45
10.1 Scorecard Metrics 45
10.2 Daily Reports 45

Appendix A. DHS Monthly FISMA Scorecard Metrics 47
A.1 Metric 1: HVA Operational Systems 49
A.2 Metric 2: Data Authorization – HVA 50
A.3 Metric 3: Non-HVA Operational Systems 51
A.4 Metric 4: Non-HVA Security Authorization 52
A.5 Metric 5: Weakness Remediation 54
A.6 Metric 6: Mandatory Unprivileged 55

A.7 Metric 7: Mandatory Privileged 56
A.8 Metric 8: Scanned Assets 57
A.9 Metric 9: Scan Compliance 58
A.10 Metric 10: Hardware Asset Management 59
A.11 Metric 11: Software Asset Management 60
A.12 Metric 12: Configuration Management 61
A.13 Metric 13: Vulnerability Management 63
A.14 Metric 14: Anti/Phishing and Malware 64
A.15 Metric 15: Network Defense 65
A.16 Metric 16: Unsupported OS 66
A.17 Metric 17: Non-TIC Connections 67
A.18 Metric 18: IOC Receiving 68
A.19 Metric 19: IDC Reporting 70

Appendix B. Scorecard Metrics Detail 72
B.1 Hardware Management Detail 73
B.2 Software Management Detail 76
B.3 Vulnerability Management Detail 79

Appendix C. Document Review Checklist 82

Appendix D. POA&M Checklist 84

Appendix E. Waivers 86

Appendix F. POA&M Reasonableness Criteria 87

Appendix G. Indicators of Compromise Scoring Criteria 88

Appendix H. Intrusion Defense Chain Scoring Criteria 90

Appendix I. DHS NIST RMF Workflow 92

Appendix J. Available Configuration Audit Files 93

Appendix K. Authorities 95

Appendix L. Acronyms and Abbreviations 96

Figures

Figure 1: Defense in Depth Layers 7
Figure 2: Phases of CDM Program 15
Figure 3: CDM Prioritization of Risk 15
Figure 4: Ongoing Authorization Process 24
Figure 5: Security Authorization Validation Process 25
Figure 6: Document Review Methodology Stages 26
Figure 7: Flaw Remediation SI-2 29
Figure 8: Media Sanitization MP-6 30
Figure 9: Physical and Environmental Protection Policy and Procedures PE-1 31

Figure 10: Configuration Management Settings CM-6 32
Figure 11: FY17 DHS Monthly FISMA Scorecard 45
Figure 12: Security Process Data Flow 46
Figure 13: Continuous Monitoring Data Flow 46
Figure 14: Sample Cover Sheet 82
Figure 15: Sample of Security Plan Checklist 82
Figure 16: Sample Contingency Plan Checklist 83
Figure 17: IOC Receiving Step 1 88
Figure 18: IOC Receiving Step 2 88
Figure 19: IOC Receiving, Final Score 89
Figure 20: IDC Reporting Step 1 90
Figure 21: IDC Reporting Step 2 90
Figure 22: IDC Reporting, Final Score 91
Figure 23: DHS NIST RMF Workflow 92

Tables

Table 1: Asset Definitions 12
Table 2: Continuous Monitoring Capability Groups 14
Table 3: Data Elements for ISCM Metrics 16
Table 4: Monthly Data Collections 44
Table 5: FY17 Metrics Overview 47
Table 6: Metric 1: HVA Operational Systems 49
Table 7: Metric 2: Data Authorization - HVA 50
Table 8: Metric 3: Non-HVA Operational Systems 51
Table 9: Metric 4: Non-HVA Security Authorization 52
Table 10: Metric 5: Weakness Remediation 54
Table 11: Metric 6: Mandatory Unprivileged 55
Table 12: Metric 7: Mandatory Privileged 56
Table 13: Metric 8: Scanned Assets 57
Table 14: Metric 9: Scan Compliance 58
Table 15: Metric 10: Hardware Asset Management 59
Table 16: Metric 11: Software Asset Management 60
Table 17: Metric 12: Configuration Management 61
Table 18: Metric 13: Vulnerability Management 63
Table 19: Metric 14: Anti-Phishing/Malware 64
Table 20: Metric 15: Network Defense 65
Table 21: Metric 16: Unsupported OS 66
Table 22: Metric 17: Non-TIC Connections 67
Table 23: Metric 18: IOC Receiving 68
Table 11: Metric 19: IDC Reporting 70
Table 24: Hardware Risk Points. 73
Table 25: Hardware Impact by Device Factor 73
Table 26: Crystal Asset Detail Report Software Asset Management 74

Table 27: Hardware Impact by System Factor 74
Table 28: Hardware Definition of Variables 75
Table 29: Software Risk Points 76
Table 30: Software Impact by Device Factor 76
Table 31: Crystal Asset Detail Report Software Asset Management 77
Table 32: Software Impact by System Factor 77
Table 33: Software Definition of Variables 78
Table 34: Vulnerability Risk Points 79
Table 35: Vulnerability Impact by Device Factor 79
Table 36: Vulnerability Asset Detail Report Columns 81
Table 37: Vulnerability by System Factor 81
Table 38: Vulnerability Definitions by Variable 81
Table 39: POA&M Checklist 84
Table 40: Resources, References, and Site Links ..... **Error! Bookmark not defined.**
Table 41: Available Configuration Audit Files 93

EXECUTIVE SUMMARY

The Annual Department of Homeland Security (DHS) Information Security Performance Plan defines performance requirements, priorities, and overall goals for DHS Components and the DHS Enterprise throughout the Fiscal Year (FY). It is a tactical interpretation of numerous strategic inputs including Federal Mandates, Interagency Standards, and DHS specific policies and initiatives. The Performance Plan outputs communicate security posture and risk at the Component and Enterprise levels for remediation and strategic decision-making.

The FY17 Performance Plan addresses an array of Information Security areas through selected Metric categories such as Inventory of Systems and Assets, Information Security Continuous Monitoring (ISCM), Weakness Management, Security Operations Center (SOC) Threat Management Maturity, and Enterprise and Chief Information Officer (CIO) initiatives. ISCM is of particular concern as DHS looks to leverage the National Protection and Programs Directorate (NPPD) Federal Network Resilience's (FNR), Continuous Diagnostics and Mitigation (CDM) Program, for purchasing and maintaining security tools and services. It is envisioned that the CDM Program will bolster capabilities across DHS and aid in morphing DHS to a more technologically uniform state.

In FY17, the focus will be to support all DHS Components, be accountable to the standards established by the Federal Information Security Modernization Act (FISMA) 2.0, and collaborate with Components to reduce risk by reporting Information Security vulnerabilities and non-compliance. This includes the incorporation of the DHS Cybersecurity Maturity Model (CyberMM) which aids in the identification of capability gaps, thereby providing inputs for allocation decisions to advance overall Enterprise security.

Awareness and visibility of our asset vulnerabilities and the diligence of our Information System management equates to better prepared Information Technology (IT) environment, and ultimately a more secure DHS.

The FY17 Performance Plan renews relevant themes that were underscored in FY16 while improving upon the effectiveness of several metrics and the inclusion of SOC Threat Management Maturity. These improvements are meant to promote more refined and accurate results and thereby provide a better understanding of the Information Security at DHS and its Components. Anti-Phishing and Malware metrics and the completeness or 'coverage' of Component scanning efforts continues to be a major focus. SOC Threat Management Maturity concentrates on Components capabilities to handle Indicators of Compromise (IOCs) and report on Security Events using the Intrusion Defense Chain (IDC) framework. The capability to handle IOCs, both on the classified and unclassified level, is critical to identify and mitigate against high confidence threats. The ability to map security events to the IDC enables Components and the Department to have a unified shared view of attack approaches, and. will provide consistency to successfully identify threat actions and countermeasures implemented to mitigate threat actions. All of the processes, requirements, and metrics described in this Performance Plan align either directly or indirectly with Federal Requirements and have been researched and incorporated in such a way as to help maintain the DHS leadership role in the Federal Government's Cybersecurity efforts.

The goal of the Performance Plan and compliance activities is to improve the security posture of systems and data. Measuring compliance with policies and regulations helps to identify vulnerabilities that can then be addressed and provides a more accurate understanding of the risk posture across the Department.

Note: Classified systems are no longer subject to this Performance Plan. For information and guidance regarding National Security Systems (NSS), see the "FY17 DHS NSS Cybersecurity Performance Plan".

1. INTRODUCTION

1.1 Purpose

The Annual Performance Plan describes requirements, priorities, and procedures applicable to Components in a given FY. Metrics and a monthly scorecard are used to gauge progress toward Departmental goals. The Performance Plan outputs also communicate security and risk posture at the Component and Enterprise levels for remediation and strategic decision-making.

The FY17 Performance Plan renews relevant themes which were underscored in FY16 while improving upon the effectiveness of several metrics. FY17 continues with measuring FISMA compliance in "success-by-percentages" format, but also markedly focuses on the role that specific risks play within the Department and how those risks impact the "cyber hygiene" of our information systems, networks, and devices. In an effort to remain impactful, FY17's scorecard will continue to be a single page dashboard of scores, with additional pages(s) dedicated to trending. While Strong Authentication by use of Personal Identification Verification (PIV) Card has always been a major priority, in FY17 DHS will target universal adoption of PIV authentication for all users.

The FY17 Performance Plan draws from several key sources and initiatives for guidance including:

- Ensuring alignment with Federal Cybersecurity Cross Agency Priority (CAP) Goals
- Addressing Government Accountability Office (GAO) High Risk Priorities
- Addressing vulnerabilities surfaced by National Cybersecurity Assessment Technical Service (NCATS) Cyber Hygiene scans

1.2 Scope

The FY17 Performance Plan applies to all DHS Components and the operational Information Systems for which they are responsible. Components are required to maintain operational systems with the Office of the Chief Information Security Officer (OCISO) Information Assurance Compliance System (IACS) and also to submit monthly scan data reflecting the security posture of their organizations to the DHS Chief Information Security Officer (CISO) for analysis. Data submissions are structured around metrics associated with overall Departmental goals.

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

Metrics are documented in Appendix A.

1.3 Audience

Any DHS Federal employee or contractor involved in IT compliance, security, architecture, and/or risk management has a responsibility to be familiar with and support the goals of the Performance Plan.

The DHS CISO is the primary owner of the Performance Plan and is responsible for managing necessary updates or modifications. The DHS CISO Council is the authorizing body for the content of the Performance Plan.

The primary output of the requirements contained in the Performance Plan are the DHS Monthly FISMA Scorecard, various canned, and ad-hoc reports. These outputs are used to communicate to senior DHS executives, such as the CIO and Chief Financial Officer (CFO), as well as oversight entities, such as the Office of the Inspector General (OIG). They also serve as the basis for FISMA reporting to the Office of Management and Budget (OMB), FNR, and Congress.

2. BACKGROUND

2.1 Working Groups and Integrated Project Teams

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

- **Compliance Working Group (CWG) –** The CWG is a forum to address issues and events related to Component FISMA Scorecard performances, FISMA Inventory, compliance, 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.
- **Joint Continuous Monitoring Working Group (JCMWG) –** The JCMWG is the interagency body for continuous monitoring collaboration, cooperation, and coordination. The JCMWG is the principal venue by which the Executive Branch synchronizes Continuous Monitoring policy.
- **Joint Cybersecurity Performance Metrics Working Group (JCPMWG) –** The JCPMWG is an interagency group led by the Federal CIO Council. The JCPMWG is responsible for the following:
  - Inventory Federal cybersecurity reporting requirements (e.g., FISMA, CAP, and Federal initiatives)
  - Propose consolidated reporting requirements for Sensitive But Unclassified (SBU) systems to take effect in FY 2017
  - Evaluate the business need for each reporting requirement
  - Apply a risk-based approach for metrics reporting and targets
- **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.

2.2 Goals and Objectives

In FY17, the Department intends to:

- Continue its security approach toward risk management through an evolved Scorecard
- Mature ISCM capabilities and effectiveness across the Enterprise
- Bolster collaboration, provide more efficient processes, and promote Enterprise-wide security tool standardization
- Ensure Components have the capability to receive IOCs at the Classified and Unclassified level

- Ensure Components have the capability to identify impactful IOCs and can successfully search for those IOCs
- Ensure Components have the basic capability to report on Security Events using the IDC framework
- Ensure timeliness of IOC handling and IDC reporting to maintain a high level of cyber situational awareness

2.3 Strategy

In addition to being a representation of 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. DHS priorities align with Federal Mandates and Interagency Standards, in addition to focusing on DHS' specific security needs.

FY17 metrics address the following activities:

- **Inventory of Systems and Assets** – Ensuring visibility and accountability for all information systems and assets such as workstations and servers, is foundational to the completeness and integrity of nearly all other metrics. Inventory metrics reflect whether Department requirements are being met comprehensively.
- **Enterprise Solutions** – Enterprise Solution metrics are not system specific, but rather measure how effectively Enterprise Security initiatives are deployed by large programs and/or entire Components. Examples for these will be the Cyber Order and Cyber Sprint of 2015, and second Cyber Order, 2016.
- **Information Security Continuous Monitoring** – ISCM metrics help to maintain an accurate picture of an organization's real-time security risk posture by consistently leveraging management tools, security controls, and prioritized risk mitigation.
- **Security Management** – Security Management metrics addresslongstanding security practices, many of which are Federal compliance requirements. This activity also addresses Ongoing Authorization (OA) efforts and how OA can use resources spent on traditional Security Authorization activities more effectively.
- **SOC Threat Management Maturity** – SOC Threat Management Maturity metrics address the capability of handling IOCs, both classified and unclassified, and reporting on security events using the IDC framework. This activity addresses the capability to process, identify and respond to threats with known IOCs. It also addresses the capability to perform basic analysis and reporting of Security Events within the IDC by mapping the discovery/identification of Events to the appropriate IDC stage. This will provide a common framework for the sharing of Threat Analysis and the effectiveness of countermeasures implemented across the department.

The metrics that make up each group are collectively used to form the DHS Monthly FISMA Scorecard. The Monthly FISMA Scorecard feeds into Component-level scorecards, reports at the system-level, and reports at the asset-level. This tiered approach maximizes

visibility into all levels of the Department's security posture. The FY17 Performance Plan is designed to target these cybersecurity activities and address where DHS is most vulnerable.

2.4 Cybersecurity Maturity Model

The DHS CyberMM is a DHS framework that represents the overall DHS Enterprise cybersecurity posture in terms of capabilities. The CyberMM helps DHS to identify capability gaps and duplications, thereby providing focus areas for allocation decisions. Insights from the framework are used to develop special instructions in annual Resource Planning Guidance that will advance overall Enterprise security.

Components mapped their current capabilities into the framework to achieve an end-to-end picture of DHS cyber maturity. The CyberMM shows a progression of Enterprise capability from "Level 1: Unprotected Cyber Assets" to "Level 5: Adaptive Cyber Defense." Figure shows how the CyberMM integrates the Defense-In-Depth (DiD) layers used by the DHS CISO to characterize the breadth, depth, and scope of capabilities needed to effectively protect the DHS Enterprise from cyber threat actors.

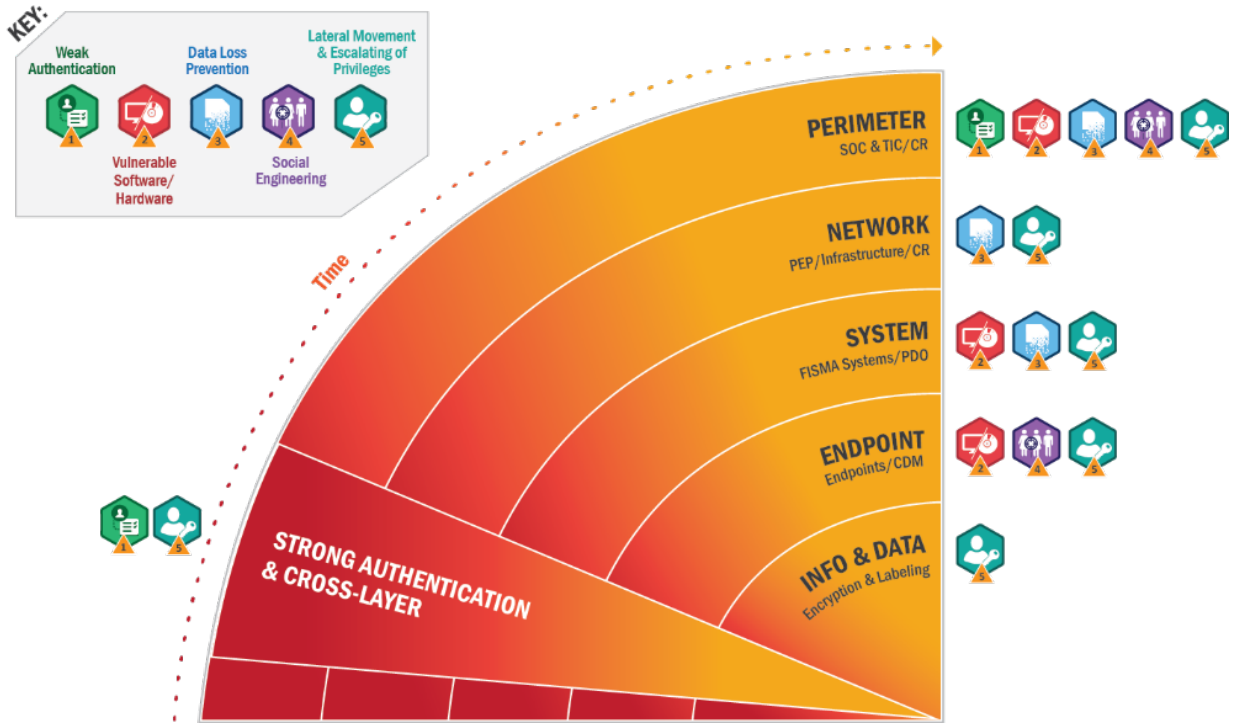


Figure 1: Defense in Depth Layers

The development of the CyberMM has provided the Department with a baseline to measure the effectiveness of capabilities and a standard lexicon and framework for evaluating Component and Enterprise Security. As a part of this assessment, Components have assessed each cyber capability area and determined a maturity level to each capability. This included the alignment of the Component's planned technologies and resources (investment data) to each capability target state. The model is currently being validated to become an evidence-based input to the next Integrated Planning Guidance. As this program matures, the Performance Plan

will incorporate the identified critical security recommendations and the effectiveness of these solutions.

3. FISMA COMPLIANCE MANAGEMENT

IACS consists of three commercial, web-based, Enterprise applications in support of the FISMA Compliance and Metrics (FCM) Division of the DHS OCISO:

- Xacta Information Assurance (IA) Assessment Engine[1],
- Continuum
- Business Objects Crystal Reports applications.

These tools are used to ensure that the Department complies with the goals and objectives establishedestablished by Federal and Agency legislation, regulations, policies, and directives including OMB, FISMA, and NIST.

IACS allows DHS to enforce FISMA compliance, as well as detect, identify, and remediate threats to system security. It will allow the Agency to assess security posture with built-in assessments using DHS 4300A and NIST 800-53 templates. Time required to complete an Authorization Package is reduced due to built-in functionality to generate Authorization documents including Requirements Traceability Matrix (RTMs), test plans, assessment and vulnerability reports, and contingency plans.

Xacta is workflow-based and uses the NIST Risk Management Framework (RMF) from start to finish. Other functions of the tool include the management of DHS Inventory for Major Applications (MAJ) and General Support Systems (GSS), capabilities to move from traditional three year Authorizations into the CISO OA Program, as well as the ability to view and leverage common controls from Federal Risk and Authorization Management Program (FedRAMP) Cloud Service Providers (CSPs).

Continuum is the Department's weakness and vulnerability management tool. Continuum contains numerous plug-ins, or means of ingesting scan data from various vulnerability scanning tools such as McAfee, Symantec, Nessus, and Retina. This scan data is aggregated into information that provides not only the Information System Security Officer (ISSO) and Information System Owner (ISO) insight into their systems' overall security posture but provides a means for analysis and scoring against the metrics defined later in this performance plan.

It is vital that DHS has an accurate accounting of all systems and assets within the Department's boundaries to determine the overall security posture of the Department. Unaccounted systems pose greater risk due to the uncertainty of ownership, maintenance, and compliance with federal mandates, directives, and policies. The goal of monitoring assets across the Enterprise is to ensure that each facet of an Information System poses the minimum risk. Ensuring security at the system level enhances security for the Enterprise.

[1] From here on out in this document, IACS refers to the application Xacta. All other applications will be called out specifically.

4. INVENTORY PROCESS

FISMA requires DHS to develop and maintain an inventory of all information systems operated by the Department. OCISO is responsible for maintaining the inventory of all Department Systems and Assets, to include Minor Applications and Subsystems, manages change control on that inventory, and assists Components in meeting compliance requirements for proper system categorization and reporting. The FISMA Inventory is the basis for many of the metrics on the scorecard and as such, it is essential that the Inventory is accurate to ensure the accuracy of the Scorecard. All procedures and requirements for requesting Inventory changes and the Annual Refresh process are described in the DHS FISMA Inventory Methodology.

In FY17, the major area of focus for Inventory will be the categorization of Cloud Systems, External Information Systems (EIS), High Value Assets (HVA), Mission Essential Systems (MES), and CFO designated systems. The Inventory Management Team (IMT) will review all systems categorized as EIS to document their use by Components and determine if any are cloud systems and should be re-categorized.

4.1 System Inventory

Accurate DHS Component system counts are the foundation upon which metrics are calculated.

In FY17 the following will continue to occur:

- Components will review and update their system Security Authorization data in IACS in a timely manner.
- Components will submit Change Requests (CRs) whenever an inventory change has occurred.
- Components will scan, monitor, and report all SBU systems and assets within their boundaries to the OCISO through the IACS Continuum Tool.

The CISO IMT will discover and maintain Components' inventories of systems through the CR process, discovery activities, and the Annual Refresh process.

4.1.1 High Value Assets

HVAs refer to those assets, systems, and data that are of particular interest to potential hackers and attackers. These assets, systems, and datasets may contain sensitive data, are used in critical operations of the Department, or house a unique collection of data (by size or content) that would make them of particular interest to criminal, politically motivated, or state-sponsored attackers.

Variables and attributes of HVAs include:

- Sensitivity of the data within the following:
  - National Security Information (NSI)
  - Controlled Unclassified Information (CUI)
  - Personally Identifiable Information (PII) & Sensitive PII (SPII)
  - Personal Health Information (PHI)

  - Federal Tax Information
  - Intellectual Property
  - Protected Critical Infrastructure Information (PCII)
  - Sensitive Security Information (SSI)
  - For Official Use Only (FOUO) – if warranted
- Amount of valued data stored:
  - Megabytes
  - Gigabytes
  - Terabytes
- Uniqueness of the dataset
  - One of a kind dataset
  - Controlled information that could be collected from other systems within the federal space
  - Uncontrolled information that could be obtained from other sources outside of the federal government
- Impact of Loss or Compromise
  - Significant Impact the Nations Security and/or populous
  - May significantly impact federal employees
  - Affects the reputation and confidence of the Department or Agency

4.1.2 Mission Essential Systems

An accurate up-to-date MES List is vital to ensuring the continuity of essential operations in the wake of a calamitous event. The MES List is a Federal priority and Components should ensure that all systems deemed mission essential are identified. The MES List is maintained by DHS Headquarters Information Technology Services Office (ITSO) Risk Management Division (RMD).

Neither non-operational systems nor EIS may be deemed essential; however, a Component may claim a system as essential if it is owned or operated by another Component, provided that the system is vital to the former's mission. Components have discretion as to which systems they determine to be mission essential provided that it's Federal Information Processing Standards (FIPS)-199 Availability rating is not "low." Systems qualifying as mission essential are added to a tracking list maintained at the Enterprise Operations Center (EOC) SharePoint Site, IACS, and the FISMA Inventory database.

4.1.3 Chief Financial Officer Designated Systems

DHS CFO Designated Systems are systems that require additional management accountability to ensure effective internal control exists over financial reporting. The DHS CFO 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 *OMB Circular No. A-123, "Management's Responsibility for Internal*

Control", Appendix A, "Implementation Guide, Internal Control over Financial Reporting. Understanding the IT Infrastructure and Associated Risks."

4.2 Asset Inventory

Components are required to report all Hardware and Software Assets within their organization in order to accurately maintain a full inventory for the ISCM Program that supports all FISMA related activities as defined by the RMF.

A Hardware Asset – often referred to as simply an "asset" in this text – is defined as:

An addressable device that can be connected to a DHS Network and used in the course of 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 Table 1. These "In-Scope Assets" represent the entire population of a Component's Hardware Asset Inventory that should be reported via the *Asset Inventory* form on the FISMA Reporting SharePoint site (see Section 8.1 Component Forms/Data Submissions). In-Scope Assets that are scanned and reported to the CISO are classified as either "Scanned" or "Invalid." "Scanned Assets" are those reporting ISCM data on a monthly basis.

Scanned Assets serve as the scoring population for ISCM metrics and are associated with a valid FISMA Identifier (ID). Invalid Assets have an invalid FISMA ID or a missing unique hostname. These two fields are "key identifiers" for all assets. All workstation and laptop devices providing an Internet Protocol (IP) address as a hostname will be considered invalid and therefore an exception. For more information on Asset Classification, see the Asset Classification White Paper

Table 1: Asset Definitions

Term	Definition	Possible Implications
In-Scope Asset	A device that is or should be connected to the unclassified network and maintains an IP address. Blackberries and other smartphones will now be included as In-Scope and report for HWAM only if they are connect to an organizational internal WI-FI network.	Should be scanned for monthly ISCM reporting and will be scored for Hardware Asset Management
Scanned Asset	A Scanned Asset that contains a valid FISMA ID and a hostname.	Scanned Assets make up the scoring population for the Scorecard and can be called 'Operational Assets' (comparable to 'Operational Systems').
Dormant Asset	Those devices that may be stored for mission related purposes and are not currently in use or assigned.	Considered 'Out of Scope' and will not be scored for any purposes. CISO will still track these devices.

Term	Definition	Possible Implications
Invalid Asset	A scanned asset that is 1) missing or has an invalid FISMA ID, 2) missing a hostname, and/or 3) is a device providing an IP address as a hostname. IP hostnames that are Dynamic Host Configuration Protocol (DHCP) create an unstable asset inventory that constantly shifts and changes.	Invalid assets cause an exception and are not imported into Continuum.
Identified Assets	A Scanned Asset that is fully defined by the Operating System (OS) Common Platform Enumeration (CPE) (e.g. Microsoft Windows 7, Solaris, CISCO Internetwork Operating System (IOS), and Windows Server 2003). These are also called "Hardware Assets."	In order to properly assign requirements to an asset, it must be identified. These assets have been credential scanned.
Unidentified Assets	A Scanned Asset that cannot define the OS CPE (e.g., (Appliances, Vendor unique devices, etc.)).	These generally result from failed or non- credentialed scans.
Software Assets	A Scanned Asset that reports Application CPEs (e.g. Java, Oracle, Internet Explorer).	The goal is to work towards creating a software asset inventory due to increasing FISMA requirements in software management and configuration.

5. INFORMATION SECURITY CONTINUOUS MONITORING

ISCM has become a leading priority at DHS and all Federal Agencies. Continuous Monitoring has also been one of the CAP Goals for the Executive Branch since 2012 and will remain as one for 2017. Continuous Monitoring provides Agencies an up-to-date picture of assets on their information networks and when their security status changes.

ISCM is a Risk Management approach that uses ongoing awareness of the security posture of IT Assets to maintain an accurate picture of organizational risk. This is accomplished through the use of automated security management tools that are able to detect, quantify, report, and potentially mitigate risks on a near-real-time basis.

5.1 Existing ISCM Capability Groups and Tools

Over the last few years, Components have been at the forefront of implementing Enterprise Continuous Monitoring Capabilities. Components have used a variety of tools to meet the technical capabilities required of an effective ISCM Program. Standardization has been encouraged by managing Enterprise License Agreements (ELA) and consolidating numerous disparate contracts and licenses across the Department. Table 2 outlines the current DHS ISCM Program. Current ISCM data collection efforts (section 5.4: ISCM Data Collection, Aggregation, and Storage) are directly aligned with Phase One of the Federal CDM Program.

Table 2: Continuous Monitoring Capability Groups

Capability Group	Description	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	Agent-based, active detection and remediation of non-compliant configurations. Capable of making changes directly to host endpoint	Tenable Nessus and/or McAfee ePO
Endpoint Protection	Agent-based solution including capabilities such as anti-virus, anti- malware, Host Based Intrusion Detection System (HID)s, and Host based Intrusion Protection (HIP)s.	McAfee ePO and Endpoint Protection Advanced tool suite and Symantec

ISCM documentation supporting these capability areas and tools can be found on the FISMA SharePoint Site and includes:

- McAfee ePO CM Reference Guide v2.2
- SOP Data Feed Submission version v5.0
- Tenable-Nessus Implementation Guide v3
- Configuration Baseline Audit Files

5.2 Continuous Diagnostics and Mitigation

The Continuous Diagnostics and Mitigation (CDM) Program provides tested continuous monitoring, diagnosis, and mitigation activities designed to strengthen the security posture of the Federal .gov networks. The CDM Program enables DHS, along with Federal Departments and Agencies (D/As), State, Local, Regional, and Tribal Governments, with the ability to enhance and further automate their existing continuous network monitoring capabilities, correlate, and analyze critical security-related information, and enhance risk-based decision making at the Agency and Federal Enterprise level.

It is envisioned that using input from the sensors and Agency-level dashboards, officials at each Agency will be able to quickly identify which problems to fix first, and empower technical managers to prioritize and mitigate risks. DHS maintains a dashboard to provide situational awareness of the Department that will feed up to the Federal level. Figure 2 shows the phases of CDM program and Figure 3 shows the prioritization of risks.

Figure 2: Phases of CDM Program

Figure 3: CDM Prioritization of Risk

The CDM Dashboard will use the RSA Archer Enterprise Governance, Risk, and Compliance (eGRC) platform which includes Federal Enterprise Management, Continuous Monitoring, and On-Demand Applications. It is envisioned that the dashboard will provide improved oversight and enhanced insight that will allow DHS to have timely situational awareness and immediate, detailed insight into cybersecurity risks and prioritize resources to focus on the most significant risks. The long term benefits include the inclusion of CDM in Federal risks scores, enable government-wide prioritization to identify potential vulnerabilities, automated reporting to address compliance requirements, and automated security controls.

While Phase One focuses on endpoint security (Managing Assets), Phase Two will address Least Privilege and Infrastructure Integrity, Phase Three will focus on boundary protection and event management, and Phase Four addresses network data protection. Currently, only Phase One is being implemented. This includes Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), and Vulnerability Management (VULN). Full implementation of CDM Phase One is expected in FY17.

5.3 ISCM Data

OMB Memorandum M-14-03 requires agencies to develop an ISCM plan and to deploy Enterprise ISCM products and services instead of multiple disparate services across Agency Bureaus/Components. While standard Enterprise tools are available to all Components, use of these tools will not be mandatory until the Department's CDM Implementation is complete. Nonetheless, there are monthly reporting standards, and the requirements of these standards are largely based on the capabilities and output formats inherent to the standard Enterprise tools.

Table 3 lists required data elements corresponding to each of the FY17 ISCM metrics. See Appendix A for corresponding metric details about these capabilities. See https://nvd.nist.gov for detailed descriptions of CPE, CVE, and CCE standards.

Table 3: Data Elements for ISCM Metrics

Capability	Requirement Data Elements
Anti-Phishing / Malware (Endpoint Protection)	• Product Version (HIPs) • Hotfix/Patch Version (HIPs) • HIPs Status • Content Version • DAT File Version • OR Date of Last Definition Update for Anti-Virus
Asset Information (applies to **all** ISCM metrics)	• FISMA ID • Hostname • CPE Standard • Device Role • Last scan date • Credentialed scan
Configuration Management	• Configuration name/version • Common Configuration Enumeration (CCE) standard • Configuration status (pass, fail, exception)

Capability	Requirement Data Elements
Software Asset Management	• CPE (application) • Accepted CPE (application) according to the Enterprise Architecture (EA) Technical Reference Model (TRM)
Vulnerability Management	• Common Vulnerability Enumeration (CVE) standard • Common Vulnerability Scoring System (CVSS) number

5.3.1 Hardware and Software Asset Management

Components are required to identify and report hardware and software assets monthly to the OCISO. A detailed list of hardware assets, to include the FISMA ID and Hostname, should be submitted monthly in order to build an accurate Asset Inventory across the Enterprise. This applies to software assets as well. In regards to the HWAM metric, several aspects of the asset submission is evaluated, to include completeness and quality. Identification of assets is key to building an accurate and functioning ISCM Program.

For an asset to be identified the following criteria must be met:

- have a valid FISMA ID
- a valid hostname
- OS CPE

Certain assets (e.g. printers, network, and communication devices) cannot report an OS CPE but can still be classified as "Identified" if their Device Role is properly annotated in the data feed and matches the Universal Device Role List. All data loaded into Continuum must provide accurate load files to support this management metric.

For SWAM, the CISO is looking to ensure that all software in the Enterprise is authorized via the DHS Enterprise Architecture (EA) Technical Reference Model (TRM) or has a waiver and not on the Federal or Agency defined "Prohibited" list. The Agency Prohibited list has been created in collaboration with EA, OCISO, and the CMWG members during the second quarter of FY17. Software that is not defined in the DHS Approved or Prohibited lists will be considered "Unapproved" until the software can be resolved with the group as a whole.

5.3.2 Vulnerability Management

Components are required to report vulnerability information for all visible workstations, servers, and virtual machines. Until the Agency matures, in conjunction with the Implementation of the Federal CDM Program, specific devices are not required to report vulnerabilities consistently (e.g., printers, appliances, Voice Over Internet Protocol (VOIP) devices, and network devices). Vulnerabilities are to be reported in Security Content Automation Protocol (SCAP) compliant format (i.e., CVE with an associated CVSS score that indicates severity). Custom Applications that do not have CVEs should request a waiver following the DHS waiver process.

Vulnerabilities will impact the Vulnerability Management metric on the scorecard. Every very non-exempt asset must report at least one CVE (regardless of CVSS) to pass the Metric and remain below the threshold of High (<50 High) and Critical (<10 Critical) vulnerabilities per

asset. CVEs published after the start of the current reporting month are not considered when assessing Critical or High vulnerabilities.

5.3.3 Configuration Management

Components must report select configuration baseline data for applicable platforms. The list of required operating systems has been determined by NPPD's FNR branch for Federal reporting purposes; however, Continuum is only configured to accept CCE SCAP format and as such, the list of applicable platforms will be tailored down for FY17 to only those that *can* produce CCE data. Configuration audit baselines are available on the CMWG SharePoint Site. All windows products are currently available in Tenable format.

Until audit baselines are published, Components are encouraged to use a Defense Information Systems Agency (DISA) Standard for those OSs and apply relevant 4300 controls. As not all platforms have defined CCE content, OCISO will *only* require OS versions listed in Appendix J: Available Configuration Audit Files for scoring purposes on the DHS Monthly Scorecard.

SCAP Compliant CCE data must be provided for each applicable asset, including a pass, fail, or exception status indicating compliance. Excepted assets are not scored.

5.3.4 Anti-Phishing/Malware

Components must demonstrate progress in implementing agent-based, endpoint protection measure by reporting whether or not certain capabilities are installed and are active on applicable endpoints (or hosts) and HIPs is enabled on all endpoints. Endpoints are defined as workstations, laptops, notebooks, and servers.

HIPs capability must be installed and active on each endpoint and must have Anti-Virus (AV) definition files updated within 90 days of the scan date for the asset. Up to date AV definitions contribute to 75% of the Anti-Phishing/Malware score and HIPs contributes to 25% of the grade.

Additional capabilities at the host level for the Anti-Phishing/Malware CAP Goal are:

- Privileged user accounts that have a technical control preventing internet access.
- Hardware assets covered by an anti-exploitation tool.
- Hardware assets that have implemented a browser-based or Enterprise-based tool to block known phishing websites and IP addresses.

5.3.5 Information Security Vulnerability Management

The Information Security Vulnerability Management (ISVM) process focuses on ensuring that DHS Security Operations Center (SOC) ISVM messages are properly addressed across the Department. This process verifies compliance at the asset level through the vulnerability data submitted to OCISO in order to determine that vulnerabilities have been mitigated. No additional reporting is required by Components in order for this to be tracked. Please note that Component ISSOs will still continue to respond to ISVM messages and verify compliance in EOC Online. Reports on ISVM Compliance will still be issued throughout FY17 but will no longer be on the Scorecard.

5.4 ISCM Data Collection, Aggregation, and Storage

Recommended data flow for ISCM metrics begins with raw data imported into the Continuum Tool. All scan data should be uploaded to Continuum no later than the last day of the current reporting month. The data is pulled nightly to the DHS Information Assurance Repository (DIAR), which supports all DHS CISO reporting, where it is evaluated and assigned risk.

The monthly DHS FISMA Scorecard will be drafted after the first day of the month after all data has been imported into Continuum and the data pulled to DIAR. Submissions to Continuum will no longer be accepted after the last day of the month in order to deliver the DHS Monthly FISMA Scorecard in a timely manner.

Corrections can only be accepted up to two days after the draft DHS Monthly FISMA Scorecard is released. All reports are consolidated by the CISO ISCM team for analysis and used in Component daily reports, FISMA Reporting, Cyberscope, and the DHS Monthly FISMA Scorecard as appropriate.

6. SECURITY MANAGEMENT METRICS

Security Management metrics account for established and generally well-understood security practices. Many of these metrics were foundational to the initial development of the Information Security Program at DHS and remain essential to meeting Federal compliance mandates (e.g. FISMA and OMB Circulars). The DHS CISO is responsible for the collection, validation, verification, and reporting of this information both internal and external to the Department. The CISO provides tools, guidance, and Subject Matter Expertise (SME) to ensure that all Components are able to meet applicable requirements. With the integration of new technology and best practices such as ISCM, cloud computing, and security control inheritance the customary ways of addressing these areas of security are gradually transforming.

This section describes the applicable metrics and initiatives that are already affecting or will likely affect them in the future. A significant initiative is to reduce the amount of duplicative effort and cost oftentimes 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. In FY17, OA will take more of a role in transitioning to a better risk management approach.

6.1 Security Authorization

The SA process is vital to ensuring that security procedures for all operational DHS Systems are properly documented, validated, and updated on a regular basis. The Department currently requires that systems submit updated SA documentation to CISO for review at a maximum of every three years in order to obtain validation of the System's Authorization package. The CISO performs a comprehensive Document Review (DR) process to verify compliance with FISMA, NIST, and DHS requirements and provides a recommendation for initial or continued operation of the system.

Components must have a valid Authorization for each applicable system to remain compliant with DHS and Federal requirements. A valid Security Authorization is also a requirement of OA.

To achieve a valid Authorization, the following documents must be completed and validated through the DR process:

A System Authorization Package includes:

- Contingency Plan (CP)
- Contingency Plan Test (CPT) (yearly)
- Privacy Impact Assessment (if applicable)
- Privacy Threshold Analysis
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Security Plan (must be addressed yearly for CFO-designated Systems)
- Signed Accreditation Decision Letter (ATO)
- Systems of Record Notice (if applicable)

Privacy documentation was previously managed and scored separately from the Authorization Package however, due to the IACS workflow and regulations, all Privacy requirements, to include the Privacy Controls, must be met in order for the Authorization workflow to progress to the OCISO validation stage. The IACS workflow has been changed to require a successful document review before an ATO can be signed. An ATO cannot be completed or signed prior to Privacy adjudication and DHS Document Review.

6.2 Common Controls

NIST identifies three types of security controls for Information Systems that can be implemented within an organization:

1. Common controls (inherited)
2. Partially inherited (hybrid) controls
3. System-specific controls.

As defined by NIST, a security control that is provided by one organization entity (a provider) to one or more organizational Information Systems (consumers) is designated as a common control.

Security controls are inheritable by Information Systems or Information System components when the systems/components receive protection from controls that are developed, implemented, assessed, authorized, monitored, and maintained by entities other than those responsible for the system/components internal or external to the organization where the system/components reside. A collection of common controls offered by a provider is referred to as a common control program within IACS. Security controls declared in a program may be used as input to SPs for individual systems, thus reducing the documentation and implementation burden on individual system owners.

Common control programs are evaluated using a process similar to Information System evaluations. Any identified weakness found during validation testing will be captured using the DHS Management Directive 4300A, Appendix H: Plan of Action and Milestone (POA&M) Process. Common control programs should be evaluated annually. Systems within IACS that provide common controls to other systems should have their 1/3rd of their controls re-evaluated annually with all controls re-evaluated during an Authorization renewal (for those not participating in OA).

For more information on DHS Common Control initiatives or how to properly use Common Controls at your organization, contact the DHS InfoSec Customer Service Center at ISOSupport@HQ.DHS.GOV.

6.3 Ongoing Authorization

In an effort to implement a more dynamic, risk-based security authorization process, the Federal government has moved away from the static three-year Authorization requirement, which tended to only result in an accurate understanding of a System's security posture at a given moment in time, to a process of Ongoing Authorization. OA is a time-driven or event-driven Authorization process whereby the Authorizing Official (AO) is provided with the necessary and sufficient information regarding the near real-time security state of the

Information System, including the effectiveness of the security controls employed within and inherited by the System, to determine whether or not the mission/business risk of continued operation is acceptable.[2] OA differs from the periodic, three-year assessment cycle, which sometimes overlooked interim changes to a System's security posture, by requiring ongoing security assessments that continually reauthorize systems and are driven by a dynamic, risk-based evaluation as opposed to time. 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.

An effective OA program enables system-affecting risk determinations based on factors such as control effectiveness or significant system characteristic changes to be made on an ongoing basis.[3]

OA's Event-Drive Monitoring involves evaluating and testing controls when security events or "triggers" occur. Security triggers are reported in the Component's Trigger Accountability Log (TRAL) and provided to the DHS CISO OA Team on a monthly basis. Internal to each Component that is a qualification for entry into the OA program, is an Operational Risk Management Board (ORMB), composed of various SMEs, reviews each trigger to determine its impact on security controls and risk to the System. Following ORMB review, depending on trigger severity and risk to the system, the Component CISO prepares a formal letter to the AO recommending whether or not to maintain the Authorization.

Key concepts of the OA Program consist of:

- Non-compliance thresholds for both suspension of the OA process and requirement or a system to revisit parts of or the entire Authorization process.
- Self-determination of monitoring frequencies for each security control, based on system-specific characteristics.
- The establishment of remediation and escalation processes for control failures and/or incidents.
- The inclusion of continuous monitoring capabilities, Common Control Catalogs (CCC), and adequate resource allocation to system or program level OA eligibility criteria.
- Training and documenting guidance for the ISSOs to ensure understanding of new responsibilities.

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

[3] NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems", Appendix F

Although some aspects of OA remain in development and certain OA Methodology concepts are continuously being evaluated, the DHS CISO OA Team has established the following requirements for entry into the OA Program:

Components must have the following:

- Demonstrated ability to produce robust, comprehensive, and consistent ISCM data for 80% of its systems encompassing requirements specified by OMB and the DHS CISO for data collection and metrics as outlined in the document.
- Approved Common Control Catalog(s)
- OA Manager(s) must be designated in writing and completed DHS OA training.
- Chartered ORMB
- A written commitment to enter all Component systems into the OA Program within a timely manner.

Each system must have the following:

- Approved Control Allocation Table (CAT) and OA Recommendation Letter.
- Authorization package in which all Privacy requirements must have been met.
- Authorization package with an expiration date greater than 45 days after the system's OA admission.
- Component accepted into the OA Program.
- Demonstrated ability to produce 80% of the system's asset and configuration data in monthly ISCM Data Feeds on a continuous (monthly) basis.
- ISSO trained on OA processes.
- ISSO with collateral responsibilities that are less than 51%.

DHS CISO OA Team maintains a formal OA Methodology which is updated periodically to comply with policy, guidance, and as DHS continues to modify and refine the OA process. Details on edibility requirements and the overall OA Program requirements are discussed in the methodology, which can be found on the Ongoing Authorization SharePoint Site.

DHS Components are encouraged to explore methods of engaging in OA at their own organizations and to communicate strategies, challenges, or questions to the DHS CISO OA Team. Component systems without validated common control catalogs in FY17 may be ineligible for participation in OA.

Figure 4 shows the Ongoing Authorization process.

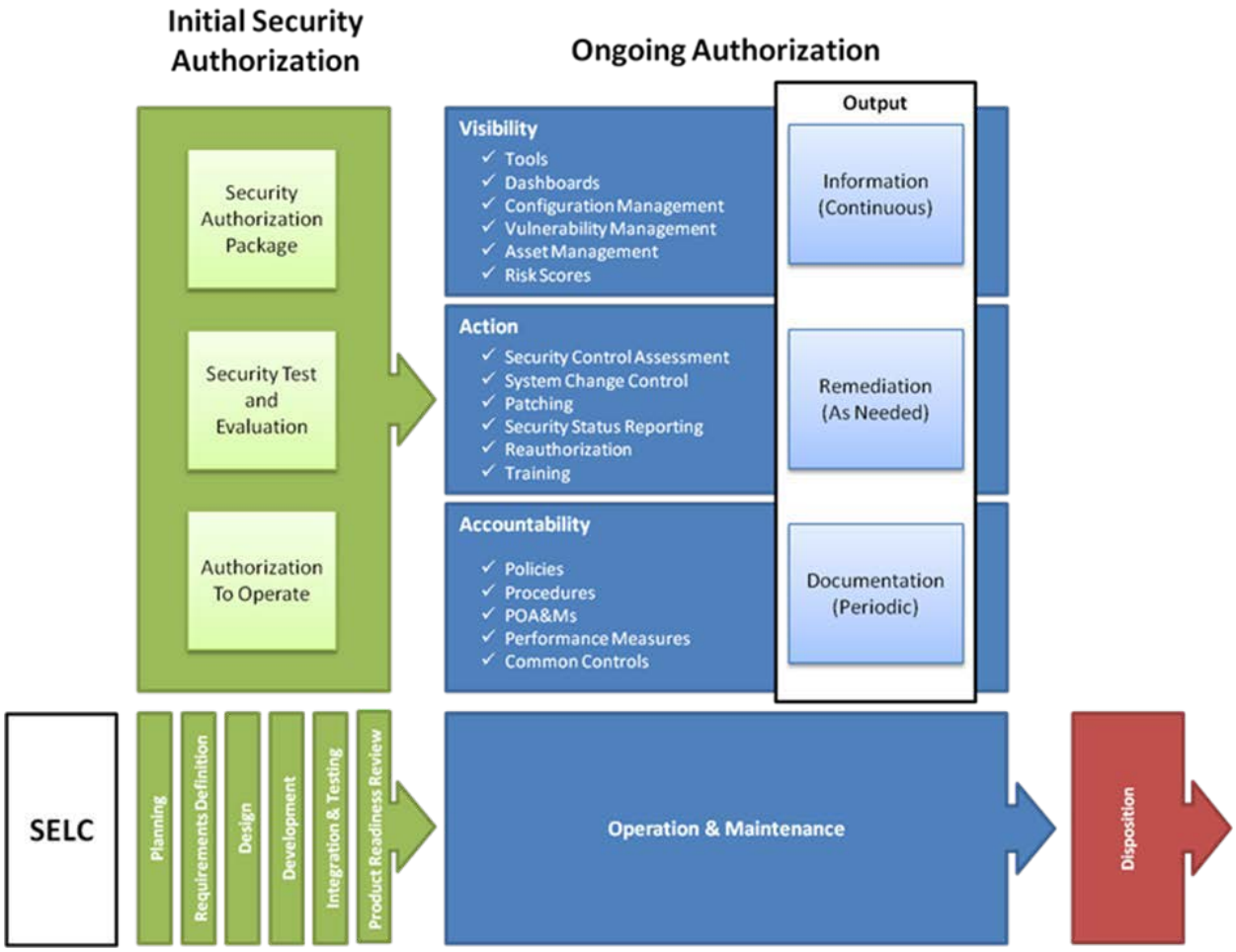


Figure 4: Ongoing Authorization Process

6.4 Document Review

The Security Authorization process is vital to verifying a System's security posture. Through comprehensive system document reviews, DHS CISO reviewers ensure that Department Systems are compliant with FISMA requirements, meet NIST DHS control implementation standards, and are eligible for initial and continued operation. The Department adheres to a maximum three-year authorization cycle policy, requiring that systems re-submit system documentation to CISO every three years to either obtain or maintain a valid Authorization. This review process is called the Document Review process.

The CISO DR Team reviews artifacts submitted as part of the SA package against a document review checklist which is described in detail in section 6.4.4 of this document. Appendix C provides where the checklist can be found and also offers screenshots to provide an idea of what the checklist looks like. The primary objective of the Document Review process is to ensure completeness and consistency with OMB and FISMA Reporting.

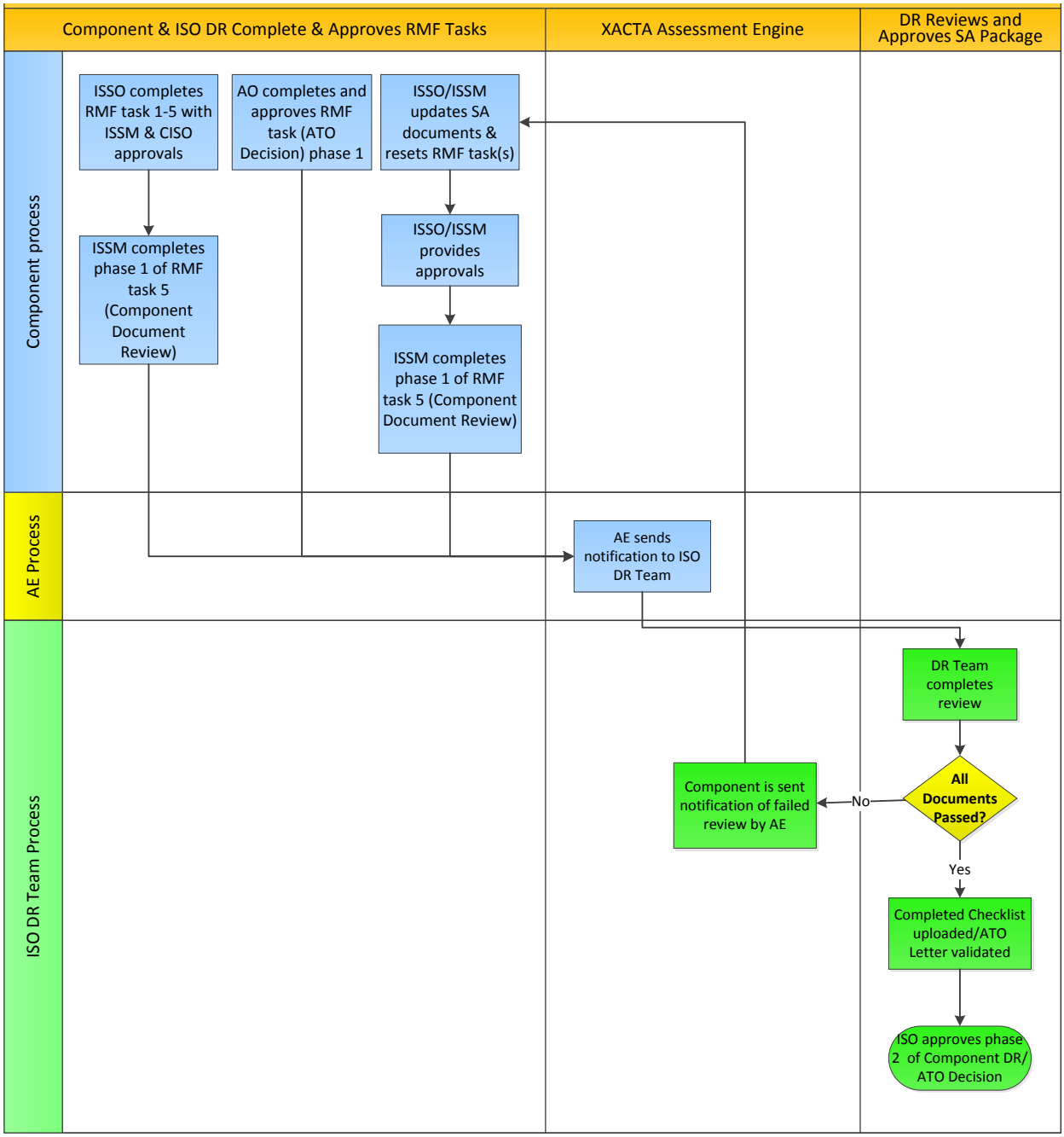


Figure 5: Security Authorization Validation Process

6.4.1 Document Review Methodology

1. The DHS Document Review Methodology is organized into four stages, described in sections 6.4.1 - 6.4.10 and summarized below. Initiation via the IACS Task Notification outlines the process for initiating the DR process for the Information Assurance Compliance System (IACS).
2. Document Review outlines the process(s) for conducting reviews whenever a notification is received.

3. Results details the criteria used by the CISO DR Team to issue a decision regarding the Checklist after a package has been reviewed and to tailor future training sessions to continually improve Component document quality.
4. Completion via the IACS Task Notification outlines the process for completing the DR process through the Information Assurance Compliance System (IACS).

Figure 6 depicts these stages.

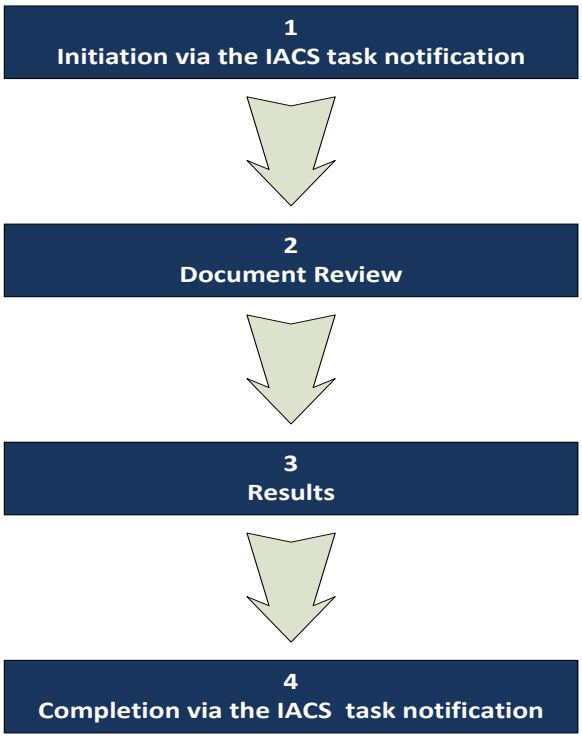


Figure 6: Document Review Methodology Stages

6.4.2 Initiation

To initiate a package review, the system ISSO, Information Security System Manager (ISSM), FISMA Compliance Team, and AO will complete Steps One through Five (ATO Decision) of the RMF Process Flow (see Appendix I). Once Step 5 (ATO Decision) has received final approval, IACS automatically sends a notification to the Certification and Accreditation Mailbox alerting the DR Team that there is a task to approve.

The DR Team receives alerts for the following types of reviews:

- Full Package Review
- Annual Contingency Plan Review (At Step 6 - Always Open Task)
- Annual Contingency Plan Test Review (At Step 6 - Always Open Task)

Packages are reviewed in the order they are received, and there is no set time frame for reviewing packages.

6.4.3 Package Categories

Due to the Workflow Process, which is the core of the IACS tool (Appendix I), Security Authorization packages can only be reviewed, approved, or disapproved as an entire package.

The Document Review Team will review the following documents:

- ATO Letter
- Contingency Plan
- Contingency Plan Test
- Privacy Impact Assessment (PIA) (for completeness if required)
- Privacy Threshold Analysis (PTA) (for completeness)
- Reliable Traceability Matrix
- Security Assessment Plan
- Security Assessment Report
- Security Plan
- Systems of Records Notice (SORN) (for completeness if required)

System personnel should upload supporting documentation, such as policy documents, Standard Operating Procedures (SOP), waivers, Memoranda of Agreements (MOA), and Service Level Agreements (SLA) into the "General Information" section of IACS. All submitted documents should be in Extensible format with the exception of the Security Assessment Plan.

6.4.4 Document Review Checklists

Reviewers employ a document review checklist for SBU system reviews to ensure that a standard set of criteria is applied uniformly across all package reviews. The checklist correlates to the security requirements of the system and is filtered based on the security categorization of the system in Step One (Categorize Information System).

For each document without a dedicated checklist, a minimum set of criteria is evaluated based on the following criteria:

- **Consistency –** The information stated in the document must be consistent across the entire package.
- **Identification –** All documents must identify with the appropriate system and system-relevant information.
- **Complete fields –** All relevant and required fields of information must be completed.
- **Signature –** When required, signature from the appropriate authorities must be present.
- **Date –** Documents must fall within the cycle of authorization in which the system is renewing or initiating.

Each control is assessed against the DHS DR Checklist and results in one of the following:

- **Pass** – The explanation of criteria are fully met.
- **Pass with comments** – The explanation of criteria are basically met but additional details are required in order to fully explain system compliance.
- **Fail** – Criteria are missing, or do not explain system-specific implementation, or provide inaccurate information and remediation/mitigation plans.
- **Not Applicable (N/A)**: Control does not apply based on system categorization and/or accreditation boundary.

6.4.5 Security Plan

Each control response is evaluated for clearness, conciseness, completeness, and correctness with regards to four criteria:

1. **What is the solution?** The solution can be a device, document, process, or plan. It must be clearly stated as the object that governs the implementation of the security control at hand.
2. **How does the solution satisfy the control or requirement?** The solution being discussed must be directly correlated to the presented requirements. It must be clear to the reviewer how the system uses the discussed solution to satisfy the requirements established by that particular security control.
3. **Who is the responsible party for solution management?** Although the ISSO may be responsible for the oversight of system security measures, a system-specific role should also be identified as managing, operating, or implementing control-relevant security measures.
4. **How frequently is the solution updated or reassessed?** Control solutions may be initiated once and continually monitored or they may require continual implementation (as is the case with revisions or updates) or a combination of the two. The timing of the solution implementation should be addressed for each requirement. A specific time frame must be provided (e.g. quarterly, monthly, every eight weeks); a response of "periodically" is not sufficient.

Section 1 of the Security Plan checklist contains information on the environment purpose, characteristics, accreditation boundary, and technologies employed within the system. Section 1 must receive a 100% pass rate for the review to continue, otherwise, it is is returned to the Component for correction.

Section 2 of the Security Plan is evaluated by randomly selecting one control family from each class of controls (management, operational, and technical). If the initial review of Section 1 yields a 10% passing rate and Section 2 yields a 90% or above passing rate; the entire Security Plan passes. If the passing rate of the three control families are below 90%, the Security Plan fails and returned to the Component for correction.

Once corrections are made and all of the approvals are completed, IACS will automatically send notification to the "Certification and Accreditation" Mailbox alerting the Document Review Team that there is a task to approve.

6.5 Documenting Implemented Controls

Figure 7 represents Flaw Remediation SI-2 as an implemented control.

Flaw Remediation	SI-2
Requirement The organization: a. Identifies, reports, and corrects information system flaws. b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation. c. Incorporates flaw remediation into the organizational configuration management process.	
Status: Implemented	
Implementation: (a) *System X* identifies system flaws through monthly scanning of system devices by the SOC using Tenable Nessus and stores the scan reports on a database server that is accessed by the ISSO via the SARGE utility tool. System Flaws are corrected by submitting proposed patches, service packs, hot fixes and updates to the CCB for approval using Remedy. (b) *System X* requires lab testing prior to controlled change release unless immediate risk requires immediate intervention. All impacted sites will be compliant within 90 days of change release. (c) *System X* incorporates flaw remediation into the organizational CM process by submitting all patches, service packs, hot fixes and updates to the CCB for approval unless there is an immediate risk requiring immediate intervention. Responsibility: The ISSO is responsible for reviewing this control at least annually or when there is a change to the Information System.	

Figure 7: Flaw Remediation SI-2

6.6 Documenting Planned Controls

Figure 8 represents Media Sanitization MP-6 as a planned control.

Media Sanitization	MP-6
Requirement The organization: a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse. b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.	
Status: Planned	
Implementation: (a) *System X* currently does not have a documented procedure for sanitizing information system media, digital nor non-digital, prior to disposal, release out of organizational control, or release for reuse. *System X* is currently drafting procedures to address this control and plans to have these procedures approved within 6 months. See POA&M # 25. (b) *System X* currently does not have a documented procedure for employing sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. *System X* is currently drafting procedures to address this control and plans to have these procedures approved within 6 months. See POA&M # 25. Responsibility: The ISSO is responsible for reviewing this control at least annually or when there is a change to the Information System	

Figure 8: Media Sanitization MP-6

When reviewing controls that are planned, the DR Team will review the POA&M(s) listed in IACS to verify the following information:

- The POA&M number in IACS matches the POA&M number listed in the Security Plan.
- The POA&M in IACS addresses the control the Security Plan claims to address.
- The POA&M status in IACS is accurate. It is not uncommon to see POA&Ms in IACS marked "Closed," but the documentation has not been updated in the Security Plan.

6.7 Documenting Control Inheritance

Systems that inherit controls from a provider system must document all partially or fully inherited controls in the appropriate security documentation. References should clearly identify which control line items are either inherited or partially inherited, the CCC title, version number, and date of publication. The Component need not provide implementation details for any control

or part of a control that is inherited, but must provide implementation details for any remaining system responsibility. See 6.2, Common Controls, for more information.

Figure 9 represents Physical and Environmental Protection Policy and Procedures PE-1 as a fully inherited control and Figure 10 represents Configuration Management Settings CM-6 as a partially inherited control.

Physical and Environmental Protection Policy and Procedures	PE-1
The organization develops, disseminates, and reviews/updates *[Assignment: organization- defined frequency]*: • A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	
Status: Fully Inherited Implementation: This control is identified as a common control and is fully inherited from DC1 (Data Center 1 Catalog version 1.1., June 28, 2011). Responsibility: The ISSO is responsible for reviewing this control at least annually or when there is a change to the Information System.	

Figure 9: Physical and Environmental Protection Policy and Procedures PE-1

Configuration Management Settings	CM-6
• Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements. • Implements the configuration settings. • Identifies, documents, and approves exceptions from the mandatory configuration settings for Individual components within the information system based on explicit operational requirements. • Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	
Status: Partially Inherited	
Implementation: This control is identified as a common control and is partially inherited from the DHS CISO Program (DHS CISO Program CCC version 0.3, April 30, 2012). System Responsibility: • [system-specific configuration settings implementation] • [system-specific identification, documentation, and exception approvals based on operational requirements details] • [system-specific monitoring and configuration changes details] Responsibility: The ISSO is responsible for reviewing this control at least annually or when there is a change to the Information System.	

Figure 10: Configuration Management Settings CM-6

6.7.1 Contingency Plan and Contingency Plan Test

The CP and CPT can only be properly developed after a business impact analysis (BIA) is conducted for the system. Although the DR Team does not review the BIA, it is an essential component of contingency planning.

The CP outlines the type of scenario to which it is meant to respond and give details on how it integrates with other, larger organizational plans such as Disaster Recovery Plans or Continuity of Operations Plans. Additionally, the CP outlines restoration procedures, identify teams and personnel involved at each stage of restoration, and define restoration objectives for each team. If a SLA, Memoranda of Understanding (MOU), or MOA are in place, they must also be referenced and discussed.

The CPT focuses on testing the plan(s) established by the CP. The level of testing is dependent upon the availability level of the system. Separate checklists and templates exist for each of the three availability levels.

6.7.2 Security Assessment Plan

The Security Assessment Plan (SAP) is evaluated to gain an understanding of how the Component plans to conduct its testing of security controls. Hardware, software, operating systems, network interfaces, and access methods are all documented and tested. Any system

components excluded from testing must be identified separately, and the Security Assessment Plan must also document all testing tools and testing methods.

6.7.3 Security Assessment Report

The Security Assessment Report (SAR) is evaluated to ensure test results are provided for each control and the appropriate mitigation steps are being implemented such as opening POA&Ms, submitting requests for risk acceptance or exceptions.

6.7.4 Requirement Traceability Matrix

The Requirement Traceability Matrix (RTM) review provides a basis for the examination of controls that are continuously monitored. If artifacts are not provided, then a detailed POA&M must be reviewed.

6.7.5 Review Results

A: All Documents Passed

If all documents pass, the DR Team will approve the "DHS Document Review" task in IACS and upload the DHS DR checklist into "Managed Project Artifacts." IACS will automatically send an approval notification to the ISSO, Alternate ISSO, and Component CISO/designee.

B: One or More Documents Fail

If one or more documents fail, the DR Team will disapprove the SA Package by reactivating the "Component Document Review" task in IACS and contact the component representative using one of the methods described below.

- IACS-Alert - The DR Team will fail the package in IACS and provide a written explanation as to why the security package failed document review.
- Upload a draft copy of DHS DR Checklist in Managed Project Artifacts section of IACS with written comments as to why the package failed.
- Via telephone or email.

Annual CP and CPT packages that are not submitted in extensible format will be rejected within IACS and a note added. . Full SA Packages cannot be rejected at this time. The DR Team will reactivate the Component Document Review Task and add a note stating why the package was returned.

6.7.6 Conference Calls

At the completion of a review, a conference call may be requested to discuss any deficiencies in documentation and to assist the Component with understanding any controls that did not pass. Conference calls are intended to help improve the long-term quality of the Authorization process and help prevent recurring issues. Reviews will not result in a conference call unless requested by the Component.

6.7.7 Re-Reviews

A document re-review is only necessary if the Component package fails its initial review. Updated documents are only assessed for those line items that failed the initial review.

All changes to the new document(s) will be cross referenced for consistency throughout the package. If changes are inconsistent with other supporting system documentation, the documents will fail review. Additionally, Component packages must have a completed SP that addresses at least 90% of their security controls in order to be considered complete. If 90% of the security controls are not addressed the Security Authorization Package will fail.

6.7.8 Component Auto-Validation

In FY17, Component individuals retain the ability to submit packages that may be validated without always being reviewed by the Document Review Team through a process called auto-validation. For a Component to be placed on or continue to be on auto-validation, they must fulfill two criteria:

- The individual submitting the Security Authorization package must be a certified attendee of CISO's Document Review training (within the past 18 months).
- The reviewer must demonstrate a 90% quality review success rate on all packages submitted the month following certification.

Components must upload the checklist in the "General Information" section for the system so it can be reviewed by the DR Team.

Despite being on auto-validation, the Document Review Team may continue to randomly inspect submitted documents. These reviews will be less frequent and done at the discretion of the Document Review Team. Once certified, the CISO Document Review team will concur on Component packages approved by the reviewer within two business days.

CISO suggests that Component personnel performing the full package reviews and checklists prior to CISO Validation be the individually certified through the Document Review process as they have a complete understanding of the CISO's expectations and document standards.

6.7.9 Privacy

The total quantity of Operational Systems with Privacy documentation that is either incomplete or unapproved by the DHS Privacy Office (PRIV) will be reflected in the Privacy Reporting documents. Required privacy documents include:

- Privacy Threshold Analysis
- Privacy Impact Assessment
- System of Records Notice

All SBU systems must complete a PTA and the Privacy Controls in the SP as part of the Authorization process. A PIA and SORN must be completed if deemed necessary by the results of the system PTA. Although the OCISO is not responsible for reviewing or validating privacy documents or controls, all required documents and controls must be accounted for during the DR process. Component Privacy Officers are responsible for the Categorization phase in the RMF

Workflow, *Appendix I*. You cannot move further through the RMF Workflow without DHS PRIV validating the privacy section. Components must ensure that all privacy documentation is validated by the DHS PRIV and accessible to the DR team prior to requesting a review. Metric requirements are incorporated into the Authorization Metric *Appendix A*.

6.7.10 Authorization Extensions

Per DHS policy, Authorizations are only valid for a maximum of three years. Any Authorization extension that exceeds this three year period will not be credited to a System in the Scorecard nor approved by the DHS CISO. Due to the IACS workflow, Authorization Extensions within the three year period must be handled correctly so as to not reset the system's tasks and validation. Submit a DHS CISO signed Authorization Extension to the CandA Mailbox for review of validity.

Note: Do not change the original ATO date nor upload the Authorization Extension into the ATO Decision Task.

The ATO is input into the system by only changing the ATO Expiration Date and uploading the document to the Managed Project Artifacts. These 3 actions are the only necessary steps once an Extension is granted:

- Email the Authorization Extension to CandA@hq.dhs.gov
- Await edits from the DR Team of the ATO Expiration date only
- Upload the document to Managed Project Artifacts

Please note, an Authorization Extension that exceeds three years (original ATO period plus the extension period), becomes an invalid package and will not receive credit for the Authorization metric.

6.8 Weakness Remediation

A POA&M documents the plan to remediate IT security vulnerabilities (i.e., 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 FISMA Scorecard measures the key aspects of POA&M effectiveness. Specifically, the metric tracks the total number of POA&Ms reported as complete, on time, and passing quality checks. The POA&M Checklist provided in *Appendix D: POA&M Checklist* as well as the POA&M Process Guide provides additional details on the POA&M criteria.

FCM Division staff are available to assist Components with developing or improving POA&Ms to ensure quality standards and scheduled completion dates are met. Components are supported through POA&M reviews which provide feedback on whether or not planned corrective actions:

- Have been properly captured in POA&Ms within the required timeframes
- Address the root cause of the IT deficiency identified
- Meet compliance criteria established in the POA&M Guide and the ISPP

Complete guidance on the DHS POA&M Process can be obtained from the POA&M Process Guide (DHS Sensitive Systems Policy Directive 4300A, Attachment H).

6.9 Cyber Hygiene Scanning

NPPD's NCATS team performs continuous scans of those IP addresses owned by the Federal Government which are exposed to the open internet. Any vulnerabilities surfaced by these scans are then reported to the Agency. DHS identifies the Components which own the affected hosts by cross referencing the IP addresses against a list of IPs provided by the Vulnerability Assessment Team (VAT). These vulnerabilities are then sent to Components in a weekly report that both identifies current vulnerabilities and tracks their mitigation over time.

6.10 CISO Security Reviews

OCISO conducts Information System reviews to meet all Federal regulatory and Organizational requirements. The CISO review team is capable of assessing nearly all Scorecard elements due to an ever-expanding breadth of focus. Reviews are conducted to assess general FISMA compliance of Component systems. Security Assessments are conducted for any system requesting a determination as to whether or not its controls are implemented and operating as intended, the impact of said controls, and countermeasures to remediate risks associated with discovered vulnerabilities.

Component Outreach and Assist Visits (COAVs) were added to the general set of security reviews in FY13 to provide CISO and Components the opportunity to have face-to-face discussions about various initiatives.

6.10.1 Component Outreach Assist Visits

The main focus for COAV includes the following tasks:

- Assist DHS Components usingthe COAV Methodology Checklist to perform ongoing assessments of Systems within OA as well as those preparing for entry into the Program.
- Customized IACS walkthrough training for ISSOs to assist with proper data entry within the following areas:
  - COAV Methodology Checklist guidance
  - POA&M Attachment H Quality check items
  - RMF guidance
  - IACS workflow items (1-6) guidance
  - IACS OA enhancements
  - Pending future recommendations from Components
  - POA&M workshops to assist in the development of timely and effective weakness remediation processes.
  - Supporting the ISO IMT in the identification and validation of Component Information System assets.

- Examining System security documentation, System security artifacts, System configuration settings, walkthrough inspection(s) of the Information System facility, and interviews with key personnel such as ISSO, technical personnel, and system owner.

COAV personnel will be called upon to perform visits to evaluate and assist with Information Security related tasks.

These tasks include:

- Identifying and documenting potential information system vulnerabilities prior to exploitation by external and internal threat agents.
- Providing recommendations and guidance in the remediation of identified vulnerabilities, prior to their discovery in formal system audits.

6.10.2 Critical Control Review

Critical Control Reviews (CCRs) are flexible reviews designed to objectively assess specific security aspects of Component Information Systems. The process is designed to be mutually constructive and provide Components with the following insights:

- The identification and documentation of potential Information System vulnerabilities prior to their exploitation by external and internal threat agents. Vulnerabilities discovered will be documented with a POA&M.
- Recommendations and guidance in the remediation of identified vulnerabilities, prior to their discovery in formal system audits (i.e., OIG audits).
- Areas of improvement in the DHS ISCM Program.
- Support of the CISO IMT in the identification and validation of Component Information System assets.

Insight into Information Security implementation that may call for revision or expansion of existing DHS CISO security policy, procedures, and guidance.

Information Systems are selected for a CCR at the discretion of the DHS and Component CISOs. Priority is given to systems of interest to senior Information Security management, mission-critical systems, high-risk systems, or a system explicitly requested for compliance evaluation.

Reviews are conducted by the CCR Team as independent verifications of controls through a variety of methods conducted at the system site:

- Examination of System configuration settings (hardware and software elements)
- Examination of System security artifacts (records, logs, certificates, and reports)
- Examination of System security documentation (policy and procedures)
- Interviews with key personnel (ISSO, technical personnel, and system owners)
- Performance and examination of automated vulnerability scans
- Walkthrough inspection of the Information System facility

Outputs of the CCR process are a set of deliverables that comprise both qualitative and quantitative analysis of an Information System's security posture. The analysis is conducted by

the CCR team following its onsite review of a system and is based on a tailored subset of NIST SP 500-53A rev 4 test cases assessed onsite.

Completed deliverables are:

- RTM: a scored and annotated matrix of control test cases.
- Findings Report: a detailed enumeration of vulnerabilities and remediation recommendations.

System stakeholders have the option to rebut or remediate findings by submitting supplemental evidence to the CCR Team within one week of the out-briefing. Rebuttal evidence must demonstrate that a finding is in error: evidence of remediation should demonstrate that a correctly identified deficiency has been remediated. In either case, satisfactory evidence will result in revised out-brief deliverables (including the adjustment of relevant scores).

7. ENTERPRISE AND CIO FISMA METRICS

Enterprise and CIO FISMA Metrics relate to the FISMA CAP Goals established by OMB in conjunction with NPPD's FNR Branch. DHS tracks and measures Components according to the requirements adopted by the governing body and reports these Metrics through Quarterly and Annual FISMA Reporting mechanisms. Section 7.1 – 7.3 address the CAP Goals according to FY17 CIO FISMA Metric standards.

7.1 Information Security Continuous Monitoring

The Continuous Monitoring CAP Goal is comprised of several areas of ISCM capabilities; Hardware and Software Asset Management, Vulnerability Management, and Configuration Management. These capabilities are the building blocks to build and maintain a robust ISCM Program. Currently these four capabilities are being implemented through the Federal CDM Program and it is expected that the capabilities provided through CDM will eventually replace these in-place capabilities. The CAP Goal measures beyond just implementation. Areas of coverage are:

- Hardware Asset Management
  - Asset current state Enterprise visibility
  - Detect and Alert of unauthorized assets
  - Mean time to detection of a new device
  - Monitored assets covered by Network Access Control (NAC) technology
- Software Asset Management
  - Detect and block unauthorized software from executing
  - Software Asset current state Enterprise Visibility
- Configuration Management
  - Audit coverage
  - Average Audit interval
- Vulnerability Management
  - Assets that are assessed using credentialed scans
  - Mean time between scans
  - Mean time to mitigate high findings

For more information see the FY17 CIO Annual FISMA Metrics v1.0.

7.2 Anti-Phishing/Malware and Other Defenses

Anti-Phishing/Malware measurement monitors capabilities at the user, asset, and Enterprise levels. Nineteen capabilities are measured that range from measuring email capabilities, Trusted Internet Connection (TIC), and hardware assets to include HIPs enablement and AV.

Below are the measurements for the CAP Goal:

- Mean time to detect a new device.

- Number of assets scanned for malware prior to an authorized remote access connection to the unclassified network.
- Number of GFE endpoints and mobile assets are covered by a software asset management capability to detect, alert, and/or block unauthorized software from executing (e.g., certificate, path, hash value, services, and behavior based whitelisting solutions).
- Number of GFE endpoints and mobile assets authorized for remote access connection to the unclassified network.
- Number of GFE endpoints covered by an anti-exploitation tool (e.g., Microsoft Enhanced Mitigation Experience Toolkit (EMET) or similar).
- Number of GFE endpoints covered by an AV solution using file reputation services, checking files against cloud-hosted, continuously updated malware information.
- Number of GFE endpoints protected by a browser-based (e.g. Microsoft SmartScreen Filter, Microsoft Phishing Filter, etc.) or enterprise-based tool to block known phishing websites and IP addresses.
- Number of Government Furnished Equipment (GFE) endpoints covered by a host-based intrusion prevention system.
- Percent of email traffic quarantined or otherwise blocked.
- Percent of inbound network traffic that passes through a web content filter, which provides anti- phishing, anti-malware, and blocking of malicious websites (e.g. fake software updates, fake antivirus offers, and phishing offers).
- Percent of incoming email traffic analyzed for detection of clickable Uniform Resource Locators (URLs), embedded content, and attachments.
- Percent of incoming email traffic analyzed for suspicious or potentially nefarious attachments opened in a sandboxed environment or detonation chamber.
- Percent of incoming email traffic analyzed using a reputation filter (to perform threat assessment of sender).
- Percent of incoming email traffic analyzed using sender authentication protocols (e.g., Domain Keys Identified Mail (DKIM), Author Domain Signing Practices (ADSP), Domain-based Message Authentication, Reporting & Conformance (DMARC), Vouch by Reference (VBR), SPF, or IP Reverse (IPREV).
- Percent of incoming email traffic passing through anti-phishing and anti-spam filtration at the outermost border mail agent or server.
- Percent of outbound communications traffic checked at the external boundaries to detect encrypted exfiltration of information (i.e., D/A's capability to decrypt/interrogate and re-encrypt).
- Percent of outgoing email traffic that enables the recipients to verify the originator using sender authentication protocols (e.g., KIM, ADSP, DMARC, VBR, SPF, and IPREV).
- Percent of privileged user network accounts that have a technical control limiting access to only trusted sites.

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

7.3 Mandatory PIV

Mandatory PIV, or Homeland Security Presidential Directive (HSPD-12), calls for a mandatory government- wide standard for secure and reliable forms of ID issued by the Federal Government to its employees and contractors for access to Federally-Controlled facilities and networks. Based upon this directive, the NIST developed Federal Information Processing Standards Publication (FIPS Pub) 201, which includes a description of the minimum requirements for a Federal PIV system.

This metric directly relates to the desired elimination of passwords and the Enterprise-level implementation of multi-factor authentication at DHS. The plan for this metric reflects the implementation schedule set by the Identity Credential and Access Management (ICAM) Program Management Office (PMO).

8. CISO GENERAL SUPPORT

The OCISO provides targeted support for any Component or employee requiring assistance in regards to use of the FISMA tool, training material, assistance with reports and metrics, working groups, and requirements. The DHS InfoSec Customer Service Center can be reached at ISOSupport@hq.dhs.gov.

8.1 Outreach and Training

The OCISO FCM Division offers Components diverse outlets for training and education, collaborative working groups, and communications channels within DHS. In FY17, CISO will develop outreach programs to assist Components with Compliance and Department initiatives. The CISO Compliance Communication Plan outlines the approach that CISO takes to ensure that all Information Security compliance stakeholders are informed on the current direction of the compliance program, strengthen internal collaboration, and increase stakeholder awareness.

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

CISO FCM is also responsible for developing, delivering, and maintaining a high-quality educational program. Classroom trainings are currently held in the following areas.

- Document Review
- Ongoing Authorization
- Performance Plan/Scorecard
- POA&M
- Telos Continuum
- Telos Xacta

Courses are taught by CISO personnel. CISO periodically schedules training which is available to people from all Components at CISO facilities. Components may also request any available training at their location.

To request training, Components should send an email to ISOtraining@hq.dhs.gov. Individuals who want to attend CISO scheduled training should respond to the training announcement or to ISOtraining@hq.dhs.gov. They will receive a confirmation via email prior to training as well as a certification of completion post-training.

8.2 Security Training

Because DHS employees and contractors are both its greatest strength and its greatest vulnerability, the DHS CISO has prioritized ensuring that employees undergo Annual IT Security Awareness training, semi-annual Privileged User training, and Anti-Phishing training as appropriate. There is currently no Department-wide standard for training; rather, it is up to the Component to ensure that the provided trainings satisfy all areas of concern for the targeted audience. As the Department moves toward a standardized training approach, review frequency and training requirements may change to be applicable across the Enterprise.

8.2.1 Annual Information Technology Security Awareness

All DHS system users, federal and contractor, are required to complete IT Security Awareness training on an annual basis. Components should keep a record of all individuals who have fulfilled their annual training requirements, including the date of completion. The percentage of users who have not fulfilled training requirements must be provided to the OCISO for the FISMA Scorecard and Annual reporting purposes using the Annual IT Security Awareness form on the FISMA Reporting SharePoint site. This may be reported on page 2 of the DHS Monthly FISMA Scorecard. See section 9.1 Component Forms/Data Submissions.

8.2.2 Privileged User Training

Users occupying roles with privileged network access and others with significant security responsibilities (e.g., ISSOs, network administrators, system administrators, System Owners, and AOs) must receive annual specialized training specific to their security responsibilities in addition to general IT Security Awareness training. Specialized security-related training must also be provided to Senior Managers, System Owners, and Project Managers.

The OCISO definition of a user with significant security responsibilities, i.e., privileged user, is defined below:

> *DHS privileged users are "personnel, contractors, or others working on behalf of DHS (i.e., . 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, for example, key management, account management, network and system administration, incident management, database administration, and web administration.[4] Privileged users constitute those performing security-relevant functions at all levels (e.g., enterprise architecture, network, and information system) within the Enterprise.[5]*

Privileged users should be reminded of the unique risks and vulnerabilities they may face or pose to the Department due to their escalated roles. It is optimal for Privileged User training to go beyond that of basic IT Security Awareness training content and focus on consequences of inappropriate actions or relaxed attention to security controls. Components needing to develop specialized training materials for privileged staff may leverage resources already in use at DHS Headquarters (HQ). Training submissions will be tracked via the FISMA Reporting SharePoint site using the Privileged User Training Form. This may be reported on page 2 of the DHS Monthly FISMA Scorecard (see section 9.1, Component Forms/Data Submissions).

[4] Policy ID 4.1.5.c DHS 4300A Sensitive Systems Policy v9.1

[5] "Account Management Role-Based Schemes," NIST 800-53A Revision 4, page F-6

9. FISMA REPORTING SHAREPOINT

In FY17, the FISMA Reporting SharePoint site will continue to play an active role in data gathering that is conducted on a monthly basis, not just for Scorecard reporting, but also for CIO Priorities and FISMA Reporting concerns. It is intended that the OCISO will track all Annual FISMA requirements throughout the FY rather than gathering all data at the end of the FY. The reason for this shift is due to the depth and breadth of information that is now covered in the annual requirements, time constraints, and ensuring data collected is valid and has integrity.

The site is open to any DHS user for read-only access. Users who support data collection or submission efforts will need to be approved by the Component's CISO or CISO designee to receive the correct permissions. To receive access, send a request to the DHS InfoSec Customer Service Center at ISOSupport@hq.dhs.gov along with any required approvals.

9.1 Component Forms/Data Submissions

Each Component has their own form page and is where all data collection efforts are held in regard to any FISMA related reporting to include the DHS Monthly FISMA Scorecard and FISMA Reporting submissions.

There are several forms that are required to be submitted on a monthly basis. Table 4 shows the most relevant forms and their descriptions. Each Component has its own page that contain its relevant forms in this table.

Table 4: Monthly Data Collections

Form	Description
Annual IT Security Awareness Training	Components are required to provide the number of network users and the total number of those users who completed training within one year of submission date. *The total number of network users should match the number of (unprivileged) network users reported for "Mandatory PIV Tracking."* This metric may is covered on the "DHS Monthly FISMA Scorecard."
Annual Privileged User Training	Components are required to submit training templates through the SharePoint site. This metric will be reported for FISMA Reporting"
Asset Inventory	Provides tracking of all DHS assets including mobile, network, and dormant devices. Specific fields on the form will be used for "In Scope" assets on the monthly Scorecard.
ISCM Waivers	This form is intended to inform OCISO of Component's FISMA Systems that are *exempt* from providing Data Feeds for ISCM reporting in the following situations only: Air-gapped, Stand-Alone, and Application FISMA Systems (no physical devices). Although these situations are exempt from the FISMA Scorecard, it does not exempt them from being scanned for vulnerabilities or configurations for database and applications. This does not exempt the system from any other reporting mechanism (i.e., OA requirements and OMB 300 scoring). In FY17, some cloud systems can apply for this form. These situations will be reviewed on a case-by-case basis.

10. DHS FISMA SCORECARD AND REPORTING

The DHS Monthly FISMA Scorecard is a management-level report that is published monthly and distributed to the CIO Council and the CISO Council. The Scorecard is the output and the measurement of requirements outlined in this document. The Department Scorecard feeds into a Component-level Scorecard, which in turn helps to create system-level reporting. Using this tiered approach maximizes visibility into all levels of the Department's security posture.

10.1 Scorecard Metrics

Appendix A provides detailed information on all Scorecard metrics and how they are calculated. Figure 11 shows a sample of the FY17 DHS Monthly FISMA Scorecard.

	COMP1	COMP2	COMP3	COMP4	COMP5	COMP6	COMP7	COMP8	COMP9	COMP10	COMP11	COMP12	Target	DHS
Security Authorization - HVA	100%	95%	100%	90%	100%	100%	79%	80%	99%	96%	81%	92%	100%	93%
Operational High Value Assets	5	10	5	40	5	5	9	12	5	78	5	8		187
Security Authorization - Other	95%	92%	95%	79%	99%	80%	93%	94%	95%	81%	96%	94%	95%	91%
Other Operational FISMA Systems	22	35	22	9	61	22	55	42	22	22	22	7		341
Weakness Remediation	90%	81%	50%	92%	92%	90%	100%	91%	79%	89%	80%	100%	90%	86%
Mandatory Unprivileged MBE	95.00%	100.00%	95.00%	94.00%	100.00%	95.00%	98.00%	97.00%	80.00%	0.00%	95.00%	94.00%	100%	86.92%
Mandatory Privileged MBE	100.00%	96.00%	100.00%	95.00%	100.00%	100.00%	96.00%	95.00%	79.00%	99.00%	100.00%	92.00%	100%	96.00%
Scanned Assets	100,000	20,000	40,000	10,000	40,000	50,000	5,000	800	20,000	60,500	10,000	9,000		365,300
Scan Compliance	95%	95%	95%	96%	100%	95%	79%	98%	98%	100%	96%	93%	95%	95%
HW Asset Management	94%	1%	94%	80%	81%	89%	37%	94%	95%	94%	96%	79%	95%	78%
SW Asset Management	80%	100%	80%	91%	89%	80%	25%	94%	80%	100%	80%	80%	95%	82%
Vulnerability Management	79%	88%	79%	93%	83%	79%	10%	94%	79%	94%	79%	80%	95%	79%
Configuration Management	90%	94%	90%	97%	93%	90%	100%	96%	90%	99%	90%	84%	95%	93%
Anti-Phishing/Malware	95%	89%	80%	79%	92%	85%	10%	5%	50%	100%	86%	99%	90%	73%
Network Defense	97%	80%	91%	100%	96%		100%	95%	96%	86%	94%	78%	95%	95%
Unsupported Software	2	0	2	11	15	2	0	0	2	92	2	0	0	128
Non-TIC Connections/Circuits	1	0	1	0	5	1	0	0	1	0	1	0	0	10
Indicators of Compromise Receiving	78%	91%	100%	0%	35%	89%	93%	95%	95%	100%	100%	100%	100%	87%
Intrusion Defense Chain Reporting	82%	100%	98%	35%	65%	93%	100%	100%	100%	98%	85%	93%	100%	90%

ARTIFICIAL DATA

Figure 11: FY17 DHS Monthly FISMA Scorecard

10.2 Daily Reports

Crystal Reports are published daily and include ISCM data available to assist Components in managing compliance and remediation efforts. The OCISO runs the regular nightly database updates, and provides updates every three hours starting at 9:00 a.m. and ending 3:00 p.m. on a daily basis. These updates will include information from IACS; Continuum, or ISCM data, is only updated nightly at this time. See Figure 12 and Figure 13 for data flow diagrams.

For manual data collections, updates are only imported into DIAR at the end of the scoring period. These reports are available in the IACS and Crystal Reports, and can be accessed

by the Component CISO and CISO designees. Additional reports are available within the FISMA Compliance Tool, IACS, for regular program management. Several variations of detail reports may be available at the Component, Program, System, or Asset level. These reports may be requested through the CISO Reporting mailbox (ISO.Reporting@hq.dhs.gov), and published to the Component's report users. If a report is required and not available or an ad-hoc report is needed, please contact ISO.Reporting@hq.dhs.gov.

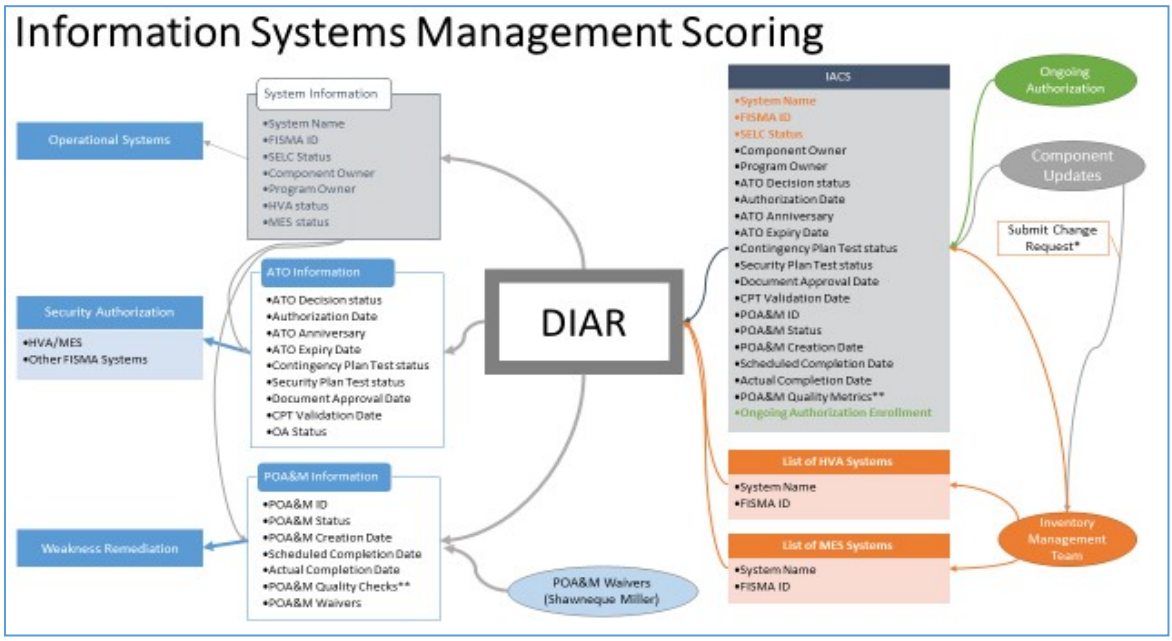


Figure 12: Security Process Data Flow

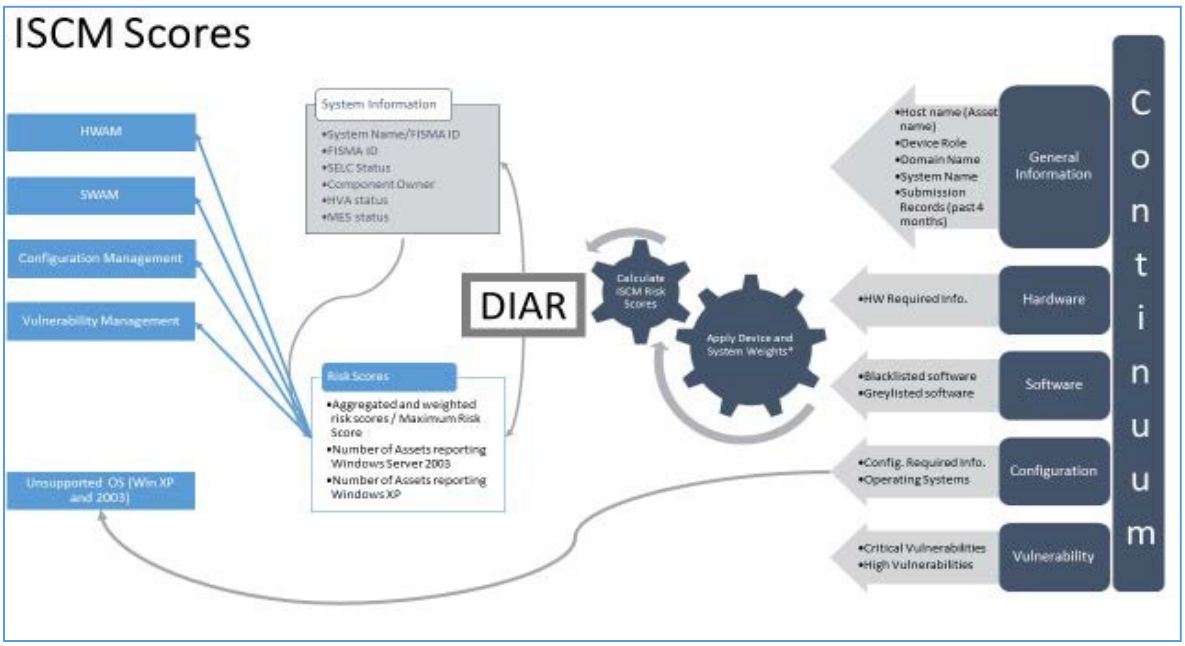


Figure 13: Continuous Monitoring Data Flow

Appendix A. DHS MONTHLY FISMA SCORECARD METRICS

The DHS FY17 Monthly FISMA Scorecard translates metric scores into percentages ranging from 0% to 100% where a higher percentage indicates a higher degree of compliance. Scorecard metrics only include SBU systems. NSS is reported in the DHS NSS Monthly FISMA Scorecard.

Table 5 lists the metrics that contribute to the DHS Monthly FISMA Scorecard. Each metric in Table 5 are described in detail throughout Appendix A.

Table 5: FY17 Metrics Overview

Metric	Description	FY17 Target
1. HVA Operational Systems	Number of the organization's HVA SBU Operational Systems	N/A
2. HVA Security Authorization	Percentage of HVA Operational systems meeting valid authorization requirements	100%
3. Non-HVA Operational Systems	Number of the organization's Non-HVA SBU Operational Systems	N/A
4. Non-HVA Security Authorization	Percentage of Non-HVA Operational systems meeting valid authorization requirements.	95%
5. Weakness Remediation	Percentage of POA&Ms meeting timelines and quality checks	90%
6. Mandatory Unprivileged	Percentage of Unprivileged network users required to use PIV card for access.	100%
7. Mandatory Privileged	Percentage of Privileged network users required to use PIV card for access	100%
8. Scanned Assets	Number of the organization's scanned assets	N/A
9. Scan Compliance	Percentage of Systems and Estimated Assets submitting scan data	95%
10. HW Asset Management	Percentage of assets with identifiable device information and role	95%
11. SW Asset Management	Percentage of applicable assets that are not running unapproved or prohibited software	95%
12. Configuration Management	Percentage of applicable assets meeting the required configuration baseline for the OS	95%
13. Vulnerability Management	Percentage of applicable assets meeting the threshold or below for high and critical vulnerabilities	95%
14. Anti-Phishing/Malware	Percentage of assets meeting endpoint security requirements	90%
15. Network Defense	Percentage of networks and assets capable of detecting, alerting, and blocking unauthorized hardware and software	95%
16. Unsupported OS	Total number of assets detected running unsupported operating systems	N/A
17. Non-TIC Connections	Total number of connections detected outside the Trusted Internet Connection	0

Metric	Description	FY17 Target
18. IOC Receiving	Percentage of capability to receive an IOC and perform enterprise wide sweeps for them	100%
19. IDC Reporting	Percentage of capability to report security events in the IDC framework	100%

A.1 Metric 1: HVA Operational Systems

Table 6 lists the fields and data of Metric 1.

Table 6: Metric 1: HVA Operational Systems

Field	Data
Metric ID	Metric 1
Metric	Number of the organizations HVA SBU Operational Systems
Type	Effectiveness
Purpose	The baseline against which Security Authorization for High Value Assets are calculated
Description	Operational Systems include GSS and MAJ in the IACS Tool with a status of "Operational," "Implementation," and "Modification." The number of Operational systems serve as the baseline for computing many metrics and it is subdivided into those systems containing High Value Assets and all other FISMA Systems. See the DHS FISMA Inventory Methodology version 13.6 for more information.
Target	N/A
Metric Calculation	Total number of SBU Operational systems in IACS that Inventory Management Team has identified as HVA
Frequency	9:00 a.m., noon, 3:00 p.m., and midnight
Responsible Parties	ISSO, ISO, CISO, and AO
Special Conditions	None
Data Source	IACS, FISMA Inventory Database
Data Quality	See section 4.1.1 High Value Assets

A.2 Metric 2: Data Authorization – HVA

Table 7 lists the fields and data of Metric 2.

Table 7: Metric 2: Data Authorization - HVA

Field	Data
Metric ID	Metric 2
Metric	Percent of HVA Operational systems meeting valid authorization requirements
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.
Description	For the purpose of this metric, a "valid" security authorization includes the following: • Completed Privacy adjudication • Completed Authorization package • Completed CPT (annually) • Completed DHS CISO Document Review • Signed ATO Letter (after CISO Doc Review) Authorization Core Documents: • Security Plan (SP) (annually for CFO- designated systems) • Security Assessment Plan (SPR) • Security Assessment Report (SAR) • Contingency Plan (CP) • Contingency Plan Test (CPT) (annually) Systems in good standing in the OA Program will receive credit for Security Authorization. The system's HVA status is derived from the FISMA Inventory Team's Database and IACS. HVA status is maintained by the Inventory Team.
Target	100%
Metric Calculation	Number of SBU Operational systems that are HVA with a valid authorization package / Number of SBU Operational systems that are HVA.
Frequency	9:00 a.m., noon, 3:00 p.m., and midnight
Responsible Parties	ISSO, ISO, AO, and Compliance Team
Special Conditions	An ATO should not be granted prior to DR Team approval and the ATO date must be on or after the DR Team's approval. Privacy must be complete prior to Component or DR Team reviews Ongoing Authorization: • Must have completed the OA Checklist, Privacy Requirements, OA Admission Letter, and the CAT Table • Ongoing Authorization Eligibility Task must be complete, ISSO approved, ISSM approved, and DHS OA Team approved. • Annual CPT complete
Data Source	IACS
Data Quality	See section 6.1 Security Authorization and 6.3 Ongoing Authorization

A.3 Metric 3: Non-HVA Operational Systems

Table 8 lists the fields and data of Metric 3.

Table 8: Metric 3: Non-HVA Operational Systems

Field	Data
Metric ID	Metric 3
Metric	Number of the organization's Non-HVA SBU Operational Systems
Type	Effectiveness
Purpose	Serves as the baseline against which Security Authorization for non-High Value Assets are calculated.
Description	Operational Systems include GSS and MAJ in IACS with a status of "Operational," "Implementation," and "Modification." The number of Operational systems serve as the baseline for computing many metrics and it is subdivided into those systems containing High Value Assets and all other FISMA Systems. See the DHS FISMA Inventory Methodology version 13.6 for more information.
Target	N/A
Metric Calculation	Total number of SBU Operational systems in IACS that Inventory Management Team has identified as non-HVA
Frequency	9:00 a.m., noon, 3:00 p.m., and midnight
Responsible Parties	ISSO, ISO, CISO, and AO
Special Conditions	None
Data Source	IACS, FISMA Inventory Database
Data Quality	See section 4.1 System Inventory

A.4 Metric 4: Non-HVA Security Authorization

Table 9 lists and fields and data of Metric 4.

Table 9: Metric 4: Non-HVA Security Authorization

Field	Data
Metric ID	Metric 4
Metric	Percent of Non-HVA Operational systems meeting valid authorization requirements
Type	Effectiveness
Purpose	DHS seeks to reduce the number of systems with invalid or out-of-date Authorization documentation. Systems approved for OA will also be included in this metric.
Description	For the purpose of this metric, a "valid" security authorization includes the following: • Completed Privacy adjudication • Completed Authorization package • Completed CPT (annually) • Completed DHS CISO Document Review • Signed ATO Letter (after CISO Doc Review) Authorization Core Documents: • Security Plan (SP) (annually for CFO- designated systems) • Security Assessment Plan (SPR) • Security Assessment Report (SAR) • Contingency Plan (CP) • Contingency Plan Test (CPT) (annually) Systems in good standing in the OA Program will receive credit for Security Authorization. The System's HVA status is derived from the FISMA Inventory Team's Database and IACS. HVA status is maintained by the Inventory Team.
Target	95%
Metric Calculation	Number of SBU Operational systems that are **not** HVA with a valid authorization package, and the number of SBU Operational systems that are not HVA.
Frequency	9:00 a.m., noon, 3:00 p.m., and midnight
Responsible Parties	ISSO, ISO, AO, and Compliance Team
Special Conditions	An ATO should not be granted prior to DR Team approval and the ATO date must be on or after the DR Team's approval. Privacy must be complete prior to Component or DR Team reviews Ongoing Authorization: • Must have completed the OA Checklist, Privacy Requirements, OA Admission Letter, and the CAT Table • Ongoing Authorization Eligibility Task must be complete, ISSO approved, ISSM approved, and DHS OA Team approved. • Annual CPT complete
Data Source	IACS

Field	Data
Data Quality	See section 6.1 Security Authorization and 6.3 Ongoing Authorization

A.5 Metric 5: Weakness Remediation

Table 10 lists the fields and data of Metric 5.

Table 10: Metric 5: Weakness Remediation

Field	Data
Metric ID	Metric 5
Metric	Percentage of POA&Ms meeting timelines and quality checks
Type	Effectiveness
Purpose	Focus will be on mitigating vulnerabilities, clean-up of POA&Ms, and addressing the GAO High Risk report.
Description	DHS monitors the number POA&Ms that fail either the quality check or management check. The Weakness Remediation metric is two-fold; Components are assessed on the percentage of incomplete, overdue, or delayed POA&Ms as well as the quality checks performed on all POA&Ms (see Appendix D: POA&M Checklist). DHS policy mandates that POA&Ms must be closed (complete) within 12 months, unless a waiver is granted by the DHS CISO and a time period for the waiver is established in the waiver. POA&Ms in IACS with a status of "Waiver" will be cross-checked with the record held by the DHS Policy team to verify the waiver and expiration date. Component Waiver are no longer accepted unless also accepted by the DHS CISO. **Note**: In addition, failure to implement any policy element within 145 days of discovery shall be considered a weakness, and a system or program POA&M must be generated All POA&Ms must have a scheduled completion date that is in the future. An open POA&M that has a scheduled completion date in the past is overdue and will fail.
Target	90%
Metric Calculation	System/Component/Department: Total number of POA&Ms passing quality and management checks and the total number of POA&Ms.
Frequency	9:00 a.m., noon, 3:00 p.m., and midnight
Responsible Parties	ISSO, ISSM, Compliance Teams, CISO Remediation Team
Special Conditions	Program POA&Ms may be open for up to five years but otherwise must pass the checks listed in Appendix D.
Data Source	IACS
Data Quality	For more information see: • Section 6.8, Weakness Remediation • Appendix D: POA&M Checks • Appendix E: Waivers • Appendix F: POA&M Reasonableness Criteria

A.6 Metric 6: Mandatory Unprivileged

Table 11 lists the field and data of Metric 6.

Table 11: Metric 6: Mandatory Unprivileged

Field	Data
Metric ID	Metric 6
Metric	Percentage of Unprivileged users required to use a PIV card for access.
Type	Implementation
Purpose	This metric determines the level of compliance with HSPD-12, which call for a government-wide secure and reliable identification standard for granting access to federally-controlled facilities, networks, and systems.
Description	Implementation goals for this metric are guided by the projected timeline established by the ICAM PMO. The ICAM PMO provides updated PIV card metrics on a weekly basis (Wednesdays) to the DHS CISO. The goal is to achieve Single Sign On (SSO) access for networks and systems.
Target	100%
Metric Calculation	Total number of Unprivileged users required to login using a PIV card and the otal number of Unprivileged users.
Frequency	Weekly
Responsible Parties	Component ICAM, ICAM PMO
Special Conditions	None
Data Source	ICAM PMO
Data Quality	Validated by ICAM PMO See section 7.3 Mandatory PIV.

A.7 Metric 7: Mandatory Privileged

Table 12 lists the field and data of Metric 7.

Table 12: Metric 7: Mandatory Privileged

Field	Data
Metric ID	Metric 7
Metric	Percent of Privileged users required to use a PIV card for access
Type	Implementation
Purpose	This metric determines the level of compliance with HSPD-12, which calls for a government-wide secure and reliable identification standard for granting access to Federally-controlled facilities and networks.
Description	Implementation goals for this metric are guided by the projected timeline establishedestablished by the ICAM PMO. The ICAM PMO provides updated PIV card metrics on a weekly basis (Wednesdays) to the DHS CISO. The goal is to achieve SSO access for networks and systems.
Target	100%
Metric Calculation	Total number of Privileged users required to use a PIV card for access and the total number of Privileged users.
Frequency	Weekly
Responsible Parties	Component ICAM, ICAM PMO
Special Conditions	None
Data Source	ICAM PMO
Data Quality	Validated by ICAM PMO See Section 7.3 Mandatory PIV.

A.8 Metric 8: Scanned Assets

Table 13 lists the field and data of Metric 8.

Table 13: Metric 8: Scanned Assets

Field	Data
Metric ID	Metric 8
Metric	Number of the Organization's scanned assets seen in Continuum
Type	Informational
Purpose	Facilitate constant and comprehensive asset visibility and an automated DHS Asset Inventory. Use Continuous Monitoring tools to properly identify every asset on a network and link it to an approved FISMA system.
Description	All addressable assets that can connect to a DHS network (to include DHS Wi-Fi networks) must be scanned for vulnerabilities and configuration settings and these scan results must be imported into the Department's Continuous Monitoring Tool, Continuum. All unique hostnames detected in scan data will be tracked as individual assets. ISSOs and Compliance Teams are responsible for maintaining this asset inventory and removing assets as they are disposed.
Target	N/A
Metric Calculation	Total number of Scanned Assets appearing in Continuum
Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, ISSMs, Compliance Teams
Special Conditions	Dormant Assets, air-gapped systems/assets, stand-alone systems/assets are considered out of scope and will require a "waiver" in order to pass the Scorecard Scan Coverage metric. These waivers will be reviewed for criteria prior to acceptance and may be subject to further reviews. Assets that have been decommissioned can be removed from Continuum and no longer be assessed toward ISCM metrics.
Data Source	Scan feeds submitted to Continuum
Data Quality	Issues that can affect the quality of this metric include: • Valid Operational FISMA ID • Valid hostname (no IP address for Workstations/Laptops) • Credentialed Scans See section 4.2: Asset Inventory for additional details.

A.9 Metric 9: Scan Compliance

Table 14 lists the field and data of Metric 9.

Table 14: Metric 9: Scan Compliance

Field	Data
Metric ID	Metric 9
Metric	Percentage of Systems and Known Assets submitting scan data
Type	Effectiveness
Purpose	Facilitate constant and comprehensive asset visibility and maintain quality standards in scan submissions.
Description	To ensure that all FISMA System Inventory and Asset Inventory is covered for Continuous Monitoring, a Scan Coverage metric is being implemented. The intention of this metric is to correlate ISCM scores with how much of an Organization's environment is scanned to be included into that score. For Systems that are air-gapped, stand-alone, or software-only FISMA Systems, the ISCM Waiver on FISMA Reporting SharePoint site can be used to show this gap and provide credit on the scorecard. For this metric to work, organizations must continuously update their Asset Inventory Form. This is not only critical for the DHS Monthly FISMA Scorecard but also for quarterly and annual FISMA Reporting cycles.
Target	95%
Metric Calculation	• **Systems**: Total number of Operational Systems providing Scan data monthly to Continuum and the total number of Operational Systems (weight 50%) + • **Assets**: Total number of scanned assets and the total number of In Scope Assets reported on FISMA SharePoint (weight 50%)
Frequency	Daily, Monthly
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	Dormant Assets, Air-gapped systems/assets, stand-alone systems/assets are considered out of scope and will require a "waiver" in order to pass the Scorecard Scan Coverage metric. These waivers are reviewed for criteria prior to acceptance and may be subject to further reviews. Assets that have been decommissioned can be removed from Continuum and no longer be assessed toward ISCM metrics.
Data Source	Scan feeds submitted to Continuum
Data Quality	See section 4.2: Asset Inventory and 9.1 Component Forms/Data Submissions for additional details.

A.10 Metric 10: Hardware Asset Management

Table 15 lists the field and data of Metric 10.

Table 15: Metric 10: Hardware Asset Management

Field	Data
Metric ID	Metric 10
Metric	Percent of Assets with identifiable device information and role
Type	Effectiveness
Purpose	Facilitate constant and comprehensive asset visibility and an automated DHS Asset Inventory. Use Continuous Monitoring tools to identify every Asset on your network and link it to an approved FISMA system.
Description	Hardware Scanned Assets measures the risk posed to a Component's assets scanned or monitored by a tool that provides OS information in CPE format. Assets submitted scan data is submitted to a quality check to assess whether the asset is identifiable to the Enterprise. Additionally, for the remainder of FY17, assets left in the Components' "Unmanaged Boundary" and not assigned to a FISMA system will be penalized on the HWAM score. For example, if 15% of the Component's assets are in the Unmanaged Boundary, 15% will be docked from the HWAM final score. This is an attempt to account for rogue/unmanaged assets within the scoring system and to emphasize assigning Assets to the correct FISMA boundary. Requirements: • Asset has been assigned a valid device role • Asset submits a valid CPE that identifies the Operating System • Asset is assigned to a defined FISMA boundary in Continuum
Target	95%
Metric Calculation	(Number of assets submitted required HWAM data elements / Total scanned assets) – (Number of Assets in Unmanaged Boundary / Total scanned assets)
Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	None
Data Source	Monthly scan feeds submitted in Continuum
Data Quality	See section 3.2: Asset Inventory See section 4.3.1: Hardware and Software Asset Management • Valid Operational FISMA ID • Valid Hostname (no IP for Workstations/Laptops) • Credentialed Scan • Valid Identification: – Operating System CPE (servers, workstations, etc.) – Device Role (Network devices, communications devices, printers, etc.) – Must match the "universal Device Role" list – Device Role will not be accepted for workstations and servers – Date last seen (Scan Date) must be within 45 days of import

A.11 Metric 11: Software Asset Management

Table 16 lists the field and data of Metric 11.

Table 16: Metric 11: Software Asset Management

Field	Data
Metric ID	Metric 11
Metric	Percent of applicable assets that are not running unapproved or prohibited software
Type	Implementation
Purpose	The FY17 goal is to build a software asset inventory in order to better understand what applications are deployed on the DHS Networks and where they are deployed.
Description	Software Asset Management will measure the risk for Component's endpoints scanned and monitored by an asset management tool that provides application data in CPE format and matches the Approved List (EA TRM). The Software Asset Management Metric describes how the risk for Component's endpoints scanned and monitored by an asset management tool will be measured. A software managed asset is any Managed Asset providing an application CPE. This metric is confined to Scanned assets that are endpoints and providing scan data within the last four months. Scanned Assets that are not an endpoint will be excluded from this metric calculation.
Target	95%
Metric Calculation	Total scanned endpoints with CPEs indicating all applications are approved software / Total scanned endpoints
Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	None applicable
Data Source	Monthly Data Feeds submitted to Continuum
Data Quality	See Section 4.2 Asset Inventory and 5.3.1 Hardware and Software Asset Management. For more information see the Asset Classification White Paper on FISMA Reporting SharePoint site. Data must include: • FISMA ID • Hostname • CPE (OS) • CPE (Application • Credentialed Scan

A.12 Metric 12: Configuration Management

Table 11 lists the field and data of Metric 12.

Table 17: Metric 12: Configuration Management

Field	Data
Metric ID	Metric 12
Metric	Percent of applicable asset OS platforms meeting the required configuration baseline for the OS
Type	Implementation
Purpose	This metric will ensure that Components are properly applying configuration baselines and monitoring their assets
Description	Components will measure the risk of assets not audited for Configuration compliance. DHS adheres to SCAP compliant content of CCEs and as such, not all platforms assessed by Federal requirements can be assessed using CCE content. See Appendix J for list of platforms. The list of OS/Versions will be confined to those types of audit files available to OS platforms and versions that will provide CCE content. Configuration Baselines are only required for those platforms supported by the Department. Specific platforms, as listed below, are required by FISMA to be audited. OCISO has created Tenable and SCAP scan profiles that can be utilized for most Windows platforms. If CISO does not have an audit file ready for Component's use, a template from nist.gov or a DISA standard that supplies CCE content can be used. Platforms that match the DHS Hardening Guidance are published on DHS Connect. The matching Automated Audit Profiles for the supported platforms can be found on the CMWG SharePoint Site. Supported platforms: Windows Vista, Windows 7x, Windows 8x, Windows 10x, Windows Server 2008, Windows Server 2012, Windows Server 2016, specific Linux, specific Unix/ Solaris, and Mac OSX. Data elements must match or contain the requirements listed in "Data Quality" section below.
Target	95%
Metric Calculation	Total applicable OS platforms/versions with valid CCEs/Total applicable OS platforms/version
Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	Previously, all Linux and Unix OS platforms were required for Configuration Management. The OCISO has condensed this list to require only versions that have an audit file available on nist.gov or within OCISO that produces CCE content successfully.
Data Source	Data Feeds submitted to Continuum

Field	Data
Data Quality	See Section 5.3.3 Configuration Management and Appendix J: Operating Systems and versions requiring Configuration. Data Elements: • FISMA ID • Hostname • CPE (OS) • Configuration Version/Name (platform version) • CCE Identifier Number – "CCE02715-1" • Configuration Status (e.g. passed, failed, waiver, or exception) • Credentialed Scan

A.13 Metric 13: Vulnerability Management

Table 18 lists the field and data of Metric 13.

Table 18: Metric 13: Vulnerability Management

Field	Data
Metric ID	Metric 13
Metric	Percent of applicable assets meeting the threshold or below for high and critical vulnerabilities
Type	Effectiveness
Purpose	This metric is to drive remediation efforts across the Department to eliminate critical vulnerabilities and raise more awareness of the vulnerabilities residing across the Department.
Description	In FY17, Components will be assessed for the risk their vulnerabilities pose to the Component and the Department as a whole. Vulnerability Management measures vulnerabilities as a percentage of applicable assets not meeting the threshold of high and critical vulnerabilities per asset. All assets must be vulnerability scanned. There are some exemptions allowed and can be found on the FISMA Reporting SharePoint site. Each asset is permitted up to 10 critical vulnerabilities and 50 high vulnerabilities. • CVSS of greater than or equal to 7 and less than 10 are considered "High" vulnerabilities (40% of score per asset) • CVSS of 10 are considered "Critical" vulnerabilities (60% of score per assets) • If applicable for vulnerability scanning and no CVEs (even low) are provided, the asset will receive 0% for vulnerability management.
Target	95%
Metric Calculation	Asset: No vulnerability scan = 0%; (applicable asset meeting threshold for High = 40%) + (applicable asset meeting threshold for Critical = 60%) Component/Department: Average Asset Score
Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	Scoring is confined to assets scanned for the current month
Data Source	Data Feeds submitted to Continuum
Data Quality	See sections 4.2 Asset Inventory and 5.3.2 Vulnerability Management for more information. Data Elements: • FISMA ID • Hostname • CVE • CVSS

A.14 Metric 14: Anti/Phishing and Malware

Table 19 lists the field and data of Metric 14.

Table 19: Metric 14: Anti-Phishing/Malware

Field	Data
Metric ID	14
Metric	Percent of assets meeting endpoint security requirements
Type	Effectiveness
Purpose	An objective of FY17 is to ensure that a) anti-virus is installed and current, and b) HIPs are installed and enabled on all endpoint devices
Description	In FY17, the Department's goal is to continue to leverage the Endpoint Security scanning capabilities supported by McAfee. Endpoint Security includes activities intended to detect and prevent propagation of malware and intrusion or unauthorized manipulation of DHS Assets. Activities in the strategic area are managed by host-based agents or applications that automatically scan, monitor, and report the status of each host. The Anti-Phishing/Malware Metric describes how the extent to which AV software has been installed and updated. This metric is confined to Identified Assets that are defined as "endpoints." In addition to ensuring AV definitions are up to date, there is an additional check to ensure HIPS is installed and enabled on the endpoint. Please note that the Department has not mandated the sole use of McAfee for endpoint reporting however, Components are expected to provide all of the same information that McAfee is capable of collecting if using a different endpoint protection tool such as Symantec.
Target	90%
Metric Calculation	Asset: Virus Definition is up to date = 75% + HIPS enabled = 25% System/Component/Department: (Total Endpoints with AV up to date / Total Endpoints) * 75% + (Total Endpoint with HIPS enabled / Total Endpoints) * 25%
Frequency	Daily
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	None applicable
Data Source	Data Feeds submitted to Continuum
Data Quality	See section 3.2 Asset Inventory and 4.3.5 Anti-Phishing/Malware for more information. Data Elements: • FISMA ID • Hostname • CPE (OS) • DAT File Version (or relative last definition update date • Product Version (HIPs) • Hotfix/Patch Version (HIPSs) • HIPS status • Content Versions • Credentialed Scan

A.15 Metric 15: Network Defense

Table 20 lists the field and data of Metric 15.

Table 20: Metric 15: Network Defense

Field	Data
Metric ID	Metric 15
Metric	% of networks and assets capable of detecting, alerting, and blocking unauthorized hardware and software.
Type	Effectiveness
Purpose	This metric is intended to improve the Department's capability of tracking and blocking unauthorized access or unauthorized software execution on the Department's networks.
Description	In FY17 DHS added this metric in order to improve the Department's Hardware and Software Asset Management CAP Goals for FISMA Reporting purposes. The Software and Hardware Defense capabilities are what is driving the Department to not meeting the CAP Goal targets. Network Defense is made up of the two sub-metrics as described below: • **Software Defense** – The percentage of the Department's endpoints and mobile assets covered by a software asset management capability to detect, alert, and/or block unauthorized software from executing (e.g., certificate, path, hash value, services, and behavior-based whitelisting solutions). • **Network Defense** – The percentage of the Department's networks having a capability or technology in place to detect and alert upon the connection of unauthorized devices.
Target	95%
Metric Calculation	Total number of endpoints and mobile devices with a capability to detect, alert, and block unauthorized software/the total number of endpoints and mobile devices (weighted 50%). Percentage of Component's network with a capability to detect and alert upon connection of unauthorized devices (weighted 50%)
Frequency	Monthly
Responsible Parties	ISSO, Data Centers, Scanning Teams, Compliance Teams
Special Conditions	None applicable
Data Source	Component FISMA data call on FISMA SharePoint Relative question numbers (5, 7, 15, and 17)
Data Quality	None

A.16 Metric 16: Unsupported OS

Table 21 lists the field and data of Metric 16.

Table 21: Metric 16: Unsupported OS

Field	Data
Metric ID	Metric 16
Metric	Total number of assets detected running unsupported operating systems
Type	Informational
Purpose	This metric is intended to track how many Department assets are running *all* End of Life (EOL) Operating Systems. Though ISCM Configuration Management scores already penalize assets for unsupported operating systems generally, EOL OS are vulnerable to particularly severe vulnerabilities and are tracked separately to maintain visibility..
Description	Unsupported Operating Systems Metric identifies how the number of Operating Systems that have reached end of life and are no longer being supported by the vendor (e.g., Windows 2003) will be measured. Because the vendor no longer provides updates or patches, these systems pose an increasing level of risk over time.
Target	0
Metric Calculation	Number of Identified assets detected with Operating Systems listed as EOL as determined by the EA TRM
Frequency	Daily (only current month data will be used)
Responsible Parties	ISSOs, Compliance Officer, OCISO
Special Conditions	As Scan data can be unreliable at properly identifying Operating System, Components will be asked to confirm the above count to ensure accuracy.
Data Source	Data Feeds submitted to Continuum
Data Quality	Scan must be credentialed A complete list of the Unsupported Operating Systems being evaluated for can be found on FISMA SharePoint.

A.17 Metric 17: Non-TIC Connections

Table 22 lists the field and data of Metric 17.

Table 22: Metric 17: Non-TIC Connections

Field	Data
Metric ID	Metric 17
Metric	Total number of connections detected outside the Trusted Internet Connection
Type	Effectiveness
Purpose	To ensure that all external connections are secured by a TIC access point in accordance with the TIC Initiative and the TIC Reference Architecture
Description	Non-TIC connections are less secure, run at great cost, and are not maximally utilized across the Department. Non-TIC Connections Metric lists the number of external network connections not secured by a TIC access point will be measured. Components are expected to reduce and consolidate all external connections through an approved TIC access point. The Department will calculate the percentage of all external traffic that is secured through a TIC access point. Cyber Hygiene Scan Reports will be monitored for new Internet connections not known to be behind the TIC.
Target	0
Metric Calculation	The number of external network connections that are not secured by a TIC access point
Frequency	Monthly
Responsible Parties	Component CISO/DHS HQ, NCATS
Special Conditions	None
Data Source	Monthly Cyber hygiene scan reports from NPPD NCATS
Data Quality	None

A.18 Metric 18: IOC Receiving

Table 23 lists the field and data of Metric 18.

Table 23: Metric 18: IOC Receiving

Field	Data
Metric ID	Metric 18
Metric	% of capability to receive an Indicator of Compromise (IOC) and perform enterprise wide sweeps for them.
Type	Operational
Purpose	This metric ensures that Components are receiving Classified and Unclassified IOCs, are capable of identifying if the IOC is impacting to their environment, and are able to perform an enterprise search for the IOC. This metric support establishing and maintaining baseline cyber health for DHS.
Description	Awareness of IOCs and the associated threats at the Component level enables sharing of critical cyber security information to improve cyber defense, incident response, and computer forensics across DHS. The capability to receive an IOC at both the Classified and Unclassified level, determining if an IOC is impactful by each Component, and the ability of Components to perform searches/sweeps as quickly as possible is critical to maintain the cyber health of DHS. IOCs are forensic artifacts of an intrusion that can be identified on a host or network. Examples of IOCs include unusual network traffic, unusual privileged user account activity, login anomalies, increases in database read volume, suspicious registry or system file changes, unusual DNS requests and Web traffic showing non-human behavior. IOCs enable Component security teams to monitor systems and networks to spot malicious actors earlier in the Intrusion Defense Chain (IDC). Classified Capability and Acknowledgement Unclassified Acknowledgement Response Action and Communication
Target	100%
Metric Calculation	• Red = 50%; Yellow = 80%; Green = 100% • Score = Average of the 5 scores below Classified capability: • Classified access: Yes or No Time of classified receipt acknowledgement: within; 24 hours, 7 days Time of unclassified receipt acknowledgement: within; 24 hours, 7 days • Response Action: Time to perform sweep or identify as non-impacting with reason: within 24 hours, 7 days Time to communicate actions: within 24 hours, 7 days
Frequency	As necessary, quarterly minimum
Responsible Parties	Security Director, SOC Branch Chief, Government Watch Officer, SOC Monitoring and Analysis Teams, Incident Response Teams
Special Conditions	None applicable
Data Source	DHS Enterprise Security Operations Center (ESOC) IOC feeds

Field	Data
Data Quality	See Appendix H for more details on scoring criteria. Data Elements: • Classified Access • Time for Acknowledgement of Classified Receipt of IOC • Time for Acknowledgement of Unclassified Receipt of IOC • Time for Determination of IOC Impact and Sweep Performed • Time for Communication of Impact and Sweep

A.19 Metric 19: IDC Reporting

Table 24 lists the field and data of Metric 19.

Table 24: Metric 19: IDC Reporting

Field	Data
Metric ID	Metric 19
Metric	% of capability to report Security Events in the Intrusion Defense Chain (IDC) framework.
Type	Operational/Reporting
Purpose	This metric ensures that Components are capable of performing base level identification and reporting of Security Events using the IDC framework. This metric support establishing and maintaining baseline cyber health for DHS.
Description	IDC identification and reporting at the Component level supports a common operational view for identification of where in the attack lifecycle an event occurred and the defensive countermeasures taken to address each stage. Components will identify base elements of the IDC to improve consistency in Security Event Identification and Remediation. The IDC is a framework used to describe a cyber-attack broken down into stages: Reconnaissance/Discovery, Weaponization, Delivery, Exploit, Installation, Command and Control (C2), and Persistence. In combating cyber-attacks, reporting of results is as important as the results. If the results can be reported in a consistent, well-structured manner, the IDC, it is possible to automate processes in detection, prevention and reporting. The following IDC elements are required for initial reporting: • IDC detection stage • Infection Source • Counter Measures Implemented • IDC stages countermeasures implemented in
Target	100%
Metric Calculation	Red = 50%; Yellow = 80%; Green = 100% Score = Average of the four scores below: • New Security Event: What phase in IDC was the event detected, Accuracy of identification • Investigation: Identification of Infection Source, Accuracy of identification • Close Event: Countermeasure implemented: time to implement (24 hours, 7 days) Event reported in IDC format: time to report (24 hours, 7 days)
Frequency	Per Event
Responsible Parties	Security Director, SOC Branch Chief, Government Watch Officer, SOC Monitoring and Analysis Teams, Incident Response Teams
Special Conditions	N/A
Data Source	Security Event Notifications (SENs), Incident Response analysis tools and processes, EOCOnline (*RSA Archer will replace EOCOnline)
Data Quality	See Appendix H for more details on scoring criteria IDC sub-set Data Elements for reporting:

Field	Data
	• Accuracy of IDC stage event detected in • Accuracy of identification of infection source • Time to implement countermeasures • IDC stage countermeasures implemented in • Time to submit IDC Security Event report

Appendix B. SCORECARD METRICS DETAIL

Although ISCM Risk scoring has been removed from the FY17 continuous monitoring metrics, OCISO will still be providing this assessment and provide the reports via the DHS FISMA Reporting Tool, Crystal Reports. Described in Appendix B1 – B4 are how the scores are broken down for Hardware Asset Management, Software Asset Management, Configuration Management, and Vulnerability Management.

The following outlines scorecard metrics:

- **Hardware Asset Management Defects**
  - Not in inventory (NII) (500 points)
  - Non-reporting (50 points)
  - Unmanaged (Rogue) (25 points)
  - Missing required information (5 points)
- **Software Asset Management (SWAM) Defects**
  - NII for required managed assets (500 points)
  - Non-reporting (50 points)
  - Software is on the Federal or Agency blacklist (25 points)
  - Software is not on the Federal or Agency blacklist or whitelist (5 points)
- **Vulnerability (VULN) Defects**
  - NII for required managed assets (1,000 points)
  - Non-reporting (100 points)
  - CVSS of 10 (10 points)
  - CVSS between 7 and 10 (5 points)
- **Configuration Settings Management (CSM)**
  - NII for required managed assets
  - Non-reporting (100 points)
  - Mission-required information (50 points)
- **By Device (Impact by Device (ImD))**
  - Server (*.2)
  - Workstation/Laptop (*.15)
  - Other (*no factor)
- **By System (Impact by System)**
  - Mission-Essential System (MES) (*.3)
  - Chief Financial Officer (CFO)/Financial (*.25)
  - Ongoing Authorization (*.2)
  - Public Facing Website (*.15)
  - Other (* no factor)

B.1 Hardware Management Detail

Purpose

Provide detailed information on the calculation of the Hardware Management Metric.

Asset Level

Calculations in Table 25 pertain to a single asset. The following risk points are assigned:

Table 25: Hardware Risk Points.

Metric Category	Risk Points
Maximum Risk Points	500
Non-Reporting Risk Points	50
Quality Risk Points	5
Un-Managed Risk Points	25

Table 26 lists the ImD factor used in formulas.

Table 26: Hardware Impact by Device Factor

Device Class	ImD Factor
Laptop	0.15
Other	0.00
Server	0.20
Workstation	0.15

The following describes the metrics:

Non-Reporting

- If no scan data has been provided in the last three months inclusive of current reporting month assign Non-Reporting Risk Points.

Quality

- Not evaluated if Non-Reporting points have already been assigned.
- Only assets reported in the current month are considered.
- If asset fails quality check assign Quality Risk Points.
- Quality = The following conditions must be met:
  - Must be credentialed scanned.
  - Non-server windows platforms must not have a hostname that is an IP address.
  - OS must be valid for Laptops, Servers, and Workstations.
  - Device Role must be valid (See current Device Role master list).
  - Last scan date must be provided and less than 30 days old.

Un-Managed

- Not evaluated if Non-Reporting points have already been assigned.
- Only assets reported in the current month are considered.
- If asset is not identified assign Un-Managed Risk Points.
- Identified = A asset is identified if matches one of the following:
  - Device class is 'Other' and OS is 'Undetermined'
  - OS is valid and Hostname is not an IP address (e.g. workstation)
  - OS is valid and Device class is 'Other' or 'Server'

Once each metric (above) is evaluated, total risk points for the asset are computed:

Asset Risk Points* = ((Non-Reporting + Quality + Un-Managed) * ImD Factor) + (Non-Reporting + Quality + Un-Managed)

Note: *Will not exceed the maximum risk points of 500.

Table 27 lists the values of the Crystal Asset Detail Report Software Asset Management columns.

Table 27: Crystal Asset Detail Report Software Asset Management

Column Name	Value
Impact by Device (ImD)	From Device Class table above
HW Non-Reporting(X = 50 pts)	Non-Reporting – calculated above
HW Unmanaged(X = 25 pts)	Un-Managed– calculated above
HW Quality(X = 5 pts)	Quality – calculated above
HWAM Score	Percentage of ((Maximum Risk Points – Asset Risk Points (*calculated above*)) / Maximum Risk Points * 100)

System Level

The following Impact by System (ImS) factor is used in the formulas in Table 28 and Table 29.

Table 28: Hardware Impact by System Factor

Sequence	Category	ImS Factor
1	Is Mission Essential	0.3
2	FIPS level is 'High' or Is CFO Designated	.25
3	Is Ongoing Authorization	0.2
4	Is Public Facing Website	.15
5	Default	0.0

Table 29: Hardware Definition of Variables

Variable	Definition
Asset Risk Points	The sum of Asset Risk Points (calculated above)
Applicable Assets	The total of all assets whose Device Role indicates it is designated as an endpoint
System Risk Points*	ROUND ((((Sum of Asset Risk Points / Sum of Applicable Assets) * ImS Factor) + (Sum of Asset Risk Points / Sum of Applicable Assets))) *Will not exceed the maximum risk points of 500.

B.2 Software Management Detail

Purpose

Provide detailed information on the calculation of the Software Management Metric.

Asset Level

The calculations below pertain to a single asset. For each of the four software metrics (NII/Non-Reporting/Prohibited/Not-Prohibited), the asset being assessed must be designated as an endpoint. This designation is determined by the asset's device role (e.g. switch, workstation, etc.).

Table 30 lists the software risk points.

Table 30: Software Risk Points

Metric Category	Risk Points
Maximum Risk Points	500
Non-Reporting Risk Points	50
Not-Prohibited (Grey list) Risk Points	5
Prohibited (Black list) Risk Points	25

The following ImD Factor is used in formulas below.

Table 31: Software Impact by Device Factor

Device Class	ImD Factor
Laptop	0.15
Other	0.00
Server	0.20
Workstation	0.15

The following describes the metrics:

- **NII**
  - Find any Application CPE in the last four months, inclusive of current reporting month.
  - If none found assign Maximum Risk Points.
- **Non-Reporting**
  - Not evaluated if NII points have already been assigned.
  - Find any Application CPE in the last three months inclusive of current reporting month.
  - If none found assign Non-Reporting Risk Points
- **Prohibited (Black list)**
  - Not currently scored
- **Not-Prohibited (Grey list)**
  - Not evaluated if NII points have already been assigned.

- Not evaluated if Non-Reporting points have already been assigned.
- Only Application CPEs in the current month are considered.
- If Not-Prohibited Application CPEs are found assign Not-Prohibited (Grey list) Risk Points

Once each metric (above) has been evaluated, total risk points for the asset are then computed:

Asset Risk Points* = ((NII + Non-Reporting + Prohibited + Not-Prohibited) * ImD Factor) + (NII + Non- Reporting + Prohibited + Not-Prohibited)

*Will not exceed the maximum risk points of 500

Table 32 lists the values of the Crystal Asset Detail Report Software Asset Management columns.

Table 32: Crystal Asset Detail Report Software Asset Management

Column Name	Value
Impact by Device (ImD)	From Device Class table above
SWAM NII(X = 500 pts)	NII – calculated above
SWAM Non-Reporting(X = 50 pts)	Non-Reporting – calculated above
Total Blacklisted Apps(Total * 25 pts)	Prohibited (Black list) – calculated above
Total Graylisted Apps(Total * 5 pts)	Not-Prohibited (Grey list) – calculated above
SWAM Risk Score	Percentage of ((Maximum Risk Points – Asset Risk Points(*calculated above*)) / Maximum Risk Points * 100)

System Level

The following ImS Factor is used in the formulas in Table 33 and Table 34.

Table 33: Software Impact by System Factor

Sequence	Category	ImS Factor
1	Is Mission Essential	.3
2	FIPS level is 'High' or Is CFO Designated	.25
3	Is Ongoing Authorization	.2
4	Is Public Facing Website	.15
5	Default	0.

Table 34: Software Definition of Variables

Variable	Definition
Asset Risk Points	The sum of Asset Risk Points (calculated above)
Applicable Assets	The total of all assets whose Device Role indicates it is designated as an endpoint
System Risk Points*	ROUND ((((Sum of Asset Risk Points / Sum of Applicable Assets) * ImS Factor) + (Sum of Asset Risk Points / Sum of Applicable Assets))) *Will not exceed the maximum risk points of 500

B.3 Vulnerability Management Detail

Purpose

Provide detailed information on the calculation of the Vulnerability Management Metric.

Asset Level

The calculations below pertain to a single asset. For each of the four vulnerability metrics (NII/Non-Reporting/Critical/High) below the asset being assessed must have the capacity to be scanned for CVEs. This capacity is determined by the asset's device role (e.g. switch, workstation, etc.)

Table 35 lists the vulnerability risk points.

Table 35: Vulnerability Risk Points

Metric Category	Risk Points
Critical Risk Points	10
High Risk Points	5
Maximum Risk Points	1000
Non-Reporting Risk Points	100

The following ImD factors is used in formulas below:

Table 36: Vulnerability Impact by Device Factor

Device Class	ImD Factor
Laptop	0.15
Other	0.00
Server	0.20
Workstation	0.15

The following is a description of the metrics:

- **NII**
  - Find any CVE in the last four months inclusive of current reporting month.
  - If none found assign Maximum Risk Points.
- **Non-Reporting**
  - Not evaluated if NII points have already been assigned.
  - Find any CVE in the last three months inclusive of current reporting month.
  - If none found assign Non-Reporting Risk Points.
- **Critical**
  - Not evaluated if NII points have already been assigned.
  - Is evaluated even if Non-Reporting points have already been assigned.
  - Only assets reported in the current month are considered.
  - Critical = (Total 'restricted' critical CVEs * Critical Risk Points)

  Note:

  A critical CVE has a CVSS equal to 10.

  'Restricted' is a CVE that is not released or updated by NIST in current month. The National Vulnerability Database (NVD) is downloaded and stored in a database and is used for determining the release and status of all CVEs.
- **High**
  - Not evaluated if NII points have already been assigned.
  - Is evaluated even if Non-Reporting points have already been assigned.
  - Only assets reported in the current month are considered.
  - High = (Total 'restricted' high CVEs * High Risk Points).

  Note:

  A high CVE has a CVSS greater than or equal to 7 and less than 10.

  'Restricted' – CVE not released or updated by NIST in current month. The NVD is downloaded and stored in a database and is used for determining the release and status of all CVEs.

Once each metric (above) has been evaluated, total risk points for the asset are then computed:

Asset Risk Points* = ((NII + Critical + High + Non-Reporting) * ImD Factor) + (NII + Critical + High + Non- Reporting)

*Will not exceed the maximum risk points of 1000.

Table 37 lists the values of the Vulnerability Asset Detail Report.

Table 37: Vulnerability Asset Detail Report Columns

Column Name	Value
Impact by Device (ImD)	From Device Class table above
Vulnerability NII(X = 1,000 pts)	NII – calculated above
Vulnerability Non-Reporting(X = 100 pts)	Non-Reporting – calculated above
Total High Vulnerabilities(Total * 5 pts)	High – calculated above
Total Critical Vulnerabilities(Total * 10 pts)	Critical – calculated above
Vulnerability Risk Score	Percentage of ((Maximum Risk Points – Asset Risk Points(*calculated above*)) / Maximum Risk Points * 100)

System Level

The following ImS factor is used in Table 38 and Table 39.

Table 38: Vulnerability by System Factor

Sequence	Category	ImS Factor
1	Is Mission Essential	.3
2	FIPS level is 'High' or Is CFO Designated	.25
3	Is Ongoing Authorization	.2
4	Is Public Facing Website	.15
5	Default	0.

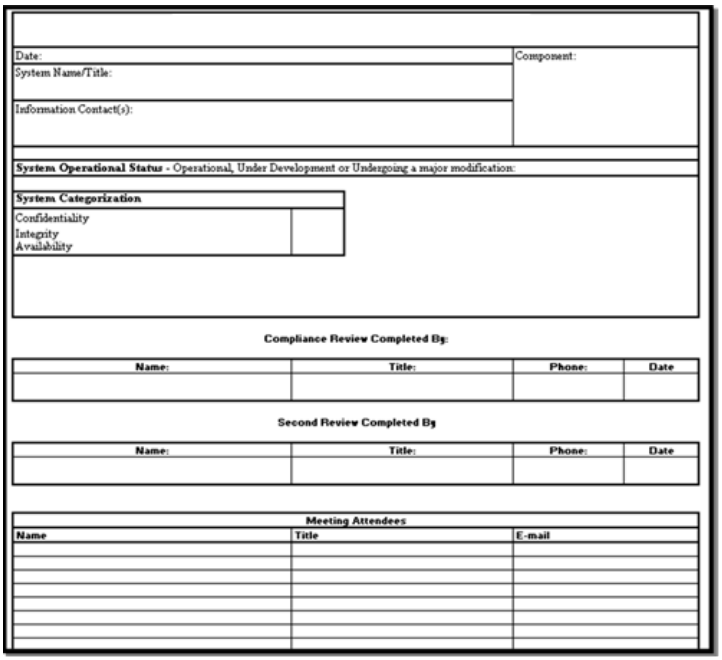
Table 39: Vulnerability Definitions by Variable

Variable	Definition
Asset Risk Points	The sum of Asset Risk Points (calculated above)
Applicable Assets	The total of all assets who's Device Role indicates the capacity for CVEs to be scanned.
System Risk Points*	ROUND ((((Sum of Asset Risk Points / Sum of Applicable Assets) * ImS Factor) + (Sum of Asset Risk Points / Sum of Applicable Assets))) *Will not exceed the maximum risk points of 1000

Appendix C. DOCUMENT REVIEW CHECKLIST

A copy of the complete checklist is available for Component use in Microsoft Excel format. The checklist can be requested from the InfoSec Customer Service Center or downloaded from the DHS CISO Website.

Figure 14 shows a sample of the DR cover sheet.



Date:	Component:
System Name/Title:	
Information Contact(s):	

System Operational Status - Operational, Under Development or Undergoing a major modification:

System Categorization	
Confidentiality	
Integrity	
Availability	

Compliance Review Completed By:

Name:	Title:	Phone:	Date

Second Review Completed By

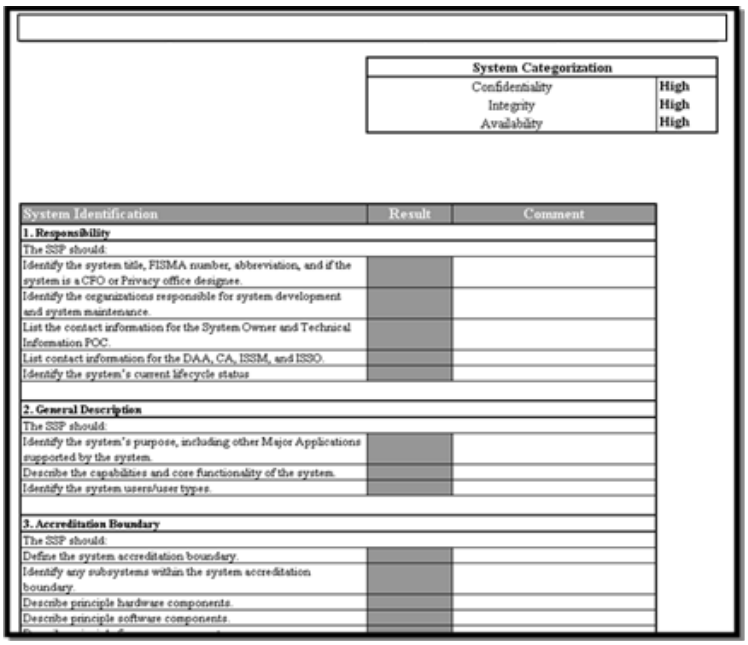
Name:	Title:	Phone:	Date

Meeting Attendees

Name	Title	E-mail

Figure 14: Sample Cover Sheet

Figure 15 shows a sample of the Security Plan checklist.



System Categorization	
Confidentiality	High
Integrity	High
Availability	High

System Identification	Result	Comment
1. Responsibility		
The SSP should:		
Identify the system title, FISMA number, abbreviation, and if the system is a CFO or Privacy office designee.		
Identify the organizations responsible for system development and system maintenance.		
List the contact information for the System Owner and Technical Information POC.		
List contact information for the DAA, CA, ISSM, and ISSO.		
Identify the system's current lifecycle status		
2. General Description		
The SSP should:		
Identify the system's purpose, including other Major Applications supported by the system.		
Describe the capabilities and core functionality of the system.		
Identify the system users/user types.		
3. Accreditation Boundary		
The SSP should:		
Define the system accreditation boundary.		
Identify any subsystems within the system accreditation boundary.		
Describe principle hardware components.		
Describe principle software components.		

Figure 15: Sample of Security Plan Checklist

Figure 16 shows a sample of the Contingency Plan checklist.

Contingency Plan Checklist

Introduction	Result	Comment
Describe the phases of the CP when a contingency event occurs		
Valid contracts or agreements with alternate sites are detailed		
The CP identifies the system components and environment to which it is applicable		
Assumptions that outline the possibilities for possible activation of the CP are detailed		
Situations for which the CP does not apply are outlined		
Reasons for the activation of the CP are described		
Requirements and references are listed		
Result for this section		

Pass
Fail
Pass with comments
N/A

Concept of Operations	Result	Comment
A detailed description of the system and its functionality is provided		
The CP describes the operating environment, physical location, general location of users, and partnerships with external organizations/systems		
Detailed backup procedures are described, including backup frequency and where tapes are stored, and responsible parties		
Preventive controls that deter, detect, or reduce system impact are discussed		
System specific technical consideration relevant to the recovery of the system are accounted for		
Network diagram is included detailing relevant system		

Figure 16: Sample Contingency Plan Checklist

Appendix D. POA&M CHECKLIST

Table 40 lists the fields of the POA&M checklist.

Table 40: POA&M Checklist

Field	Verifies
POA&M Status Check: Completed	Audit findings (selected within the "Item Identified by" field) must have an artifact uploaded to provide evidence of completion. The Component CISO approval required (TBD).
POA&M Status Check : Cancelled	Evidence signed by the AO uploaded if reason is "risk accepted" Component CISO approval required (TBD).
POA&M Status Check : Delayed	Component CISO approval required (TBD).
POA&M Status Check : Waiver	Must have a waiver signed by DHS CISO uploaded. Waiver must follow the process in DHS 4300A Appendix B. Must pass a cross check of official records with the DHS Policy Group Component approval required (TBD).
POA&M Status Check : Exception	Exceptions will be considered Open follow all requirements of an "Open" POA&M. Will reflect as "Waiver" in the DHS Reporting Tool. Must pass a cross check of official records with the DHS Policy Group Component approval required (TBD).
Point of Contact Check	Must include a name and either phone or email address
Scheduled Completion Check: System-Level POA&Ms	Dates reflect the maximum SA cycle. Scheduled completion date ≤ 12 months from creation date (may still fail under performance criteria).
Scheduled Completion Check : Program-Level POA&Ms	Scheduled completion date ≤ 5 years from creation date (may still fail under performance criteria).
Scheduled Completion Check: Waiver	Dates reflect the completion date granted on the waiver. The signed DHS CISO waiver must be loaded as an artifact to the POA&M and verified with official records with the DHS Policy Group.
Link to Control Number Check	Must include at least one NIST SP 800-53 Control. An appropriate NIST control title should be used for POA&Ms to resolve DHS MD 4300A control weaknesses. Control number should be entered manually in the weakness description field.
Item Identified During Check	At least one source is selected.
Severity Level Check	POA&Ms with the default section of "Not Assigned" will fail.
Resources Check	Meet the minimum funding resource criteria described in Appendix F. Entered in the "Resources Required" field. Must identify the source of funding and entry must match one of the following: • "currently funded" • "reallocation of resources" • "new funding request anticipated"

Field	Verifies
Milestone(s) Check	Must have at least one milestone, and \ be written as actions to address the weakness, not as a restatement of the requirement or as actions already taken. Each milestone scheduled completion date that is in the past and does not carry a status of milestone complete, will fail.
Weakness Description	Must describe the weakness in terms of what weakness needs to be resolved. It should not repeat the requirement/control description or finding.
POA&M Overdue Check	System POA&Ms must be closed within 12 months from the creation date of the POA&M. POA&Ms that have an approved/signed waiver must be closed by the Waiver Expiration Date approved by the DHS CISO. Program POA&Ms must be closed within five years from the creation date of the POA&M.
DHS CISO Approval	The CISO Office retains the ability to fail a POA&M for any manual review that finds a POA&M insufficiently address the vulnerability or is missing required descriptions or milestones.

Appendix E. WAIVERS

A waiver must be approved by the DHS CISO or designate if a system cannot meet the minimum set of security controls required by DHS 4300A Sensitive Systems Policy. The approval of a waiver is not guaranteed. If granted, the duration is set by the DHS CISO. The waiver policy is provided in section 1.5 of DHS 4300A, and the process to request a waiver is documented in the MD 4300A Sensitive Systems Handbook, Attachment B, Waiver Request Form.

Signed waivers should be uploaded into IACS as documentation before changing a POA&M status to "Waiver". Waivers will be tracked by the DHS CISO Policy Group and the DHS CISO POA&M Team outside of the IACS Tool. The data will be imported into the CISO Reporting Tool to verify POA&Ms that have a signed waiver along with the duration. POA&Ms with the status of "Waiver" will be cross-checked with the data provided by the Policy Group along with the duration of the waiver. POA&Ms that fail the cross-check will fail the POA&M Status Check as outlined in Appendix D. The status of waivers can be monitored through the DHS Reporting Tool, Crystal Reports.

Appendix F. POA&M REASONABLENESS CRITERIA

The POA&M reasonableness criteria were created to address and OIG FISMA recommendation that DHS ensure POA&Ms are reasonable to enact and is intended to deter the use of placeholder data such as $1 or $0. The criteria only checks for reasonable remediation costs (i.e., . resources). The criteria are included with Metric 5: Weakness Remediation.

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

The Reasonable Resource Matric for NIST 800-53 controls provides an estimate of the minimum resources required to remediate the specified NIST 800-53 control weakness. It is based on a nominal labor rate of $100 per hour and does not include other direct expenses (e.g., 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 (policies procedures, etc.) require a minimum of four hours or $400 to complete. The best case would be a Component or system policy.
- Configuration hardening weaknesses require a minimum of 30 minutes or $50. In some cases, only one part of a control may not be implemented. The best case could require a system administrator to close a single port or configure a setting on a server, which would take a minimal amount of time.
- Resources needed to prepare the Authorization document were based on estimated times.
- IT security controls where a cost could not be estimated due to the complexity or unknown factors (e.g., installing a fire suppression system), a nominal $5- cost has been consistently listed.

Appendix G. INDICATORS OF COMPROMISE SCORING CRITERIA

Figure 17: The Calculated Score Detail.

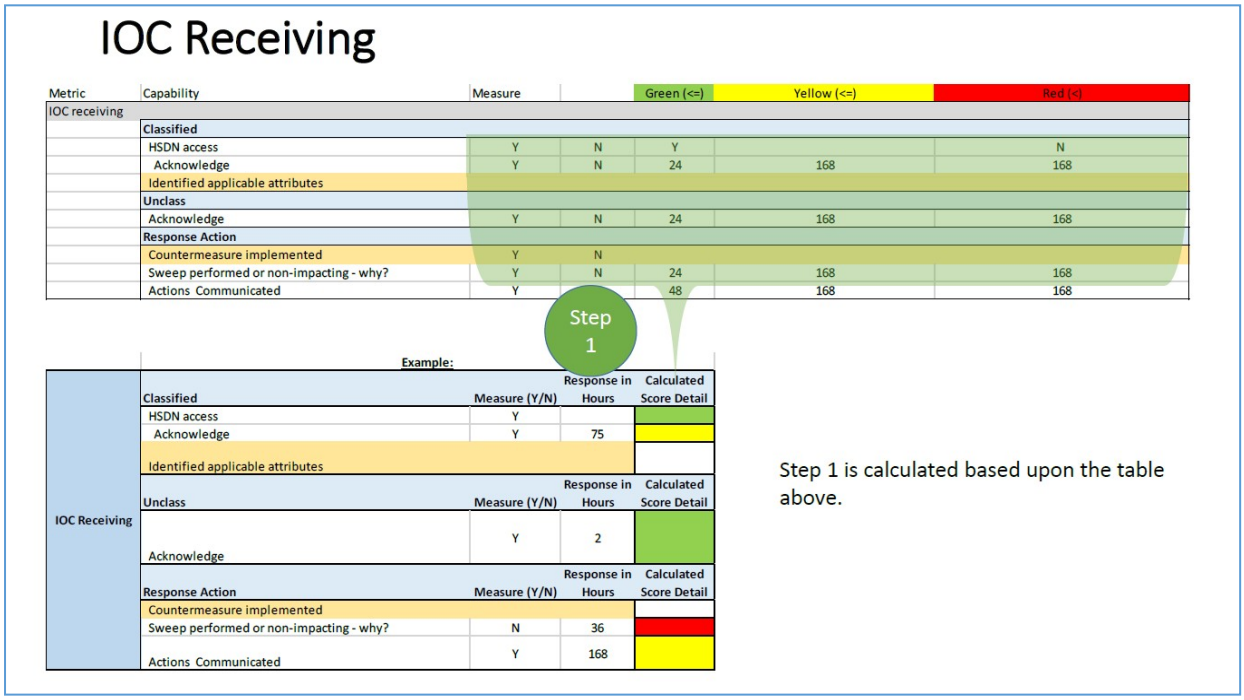


Figure 17: IOC Receiving Step 1

Figure 18: The Initial Rollup.

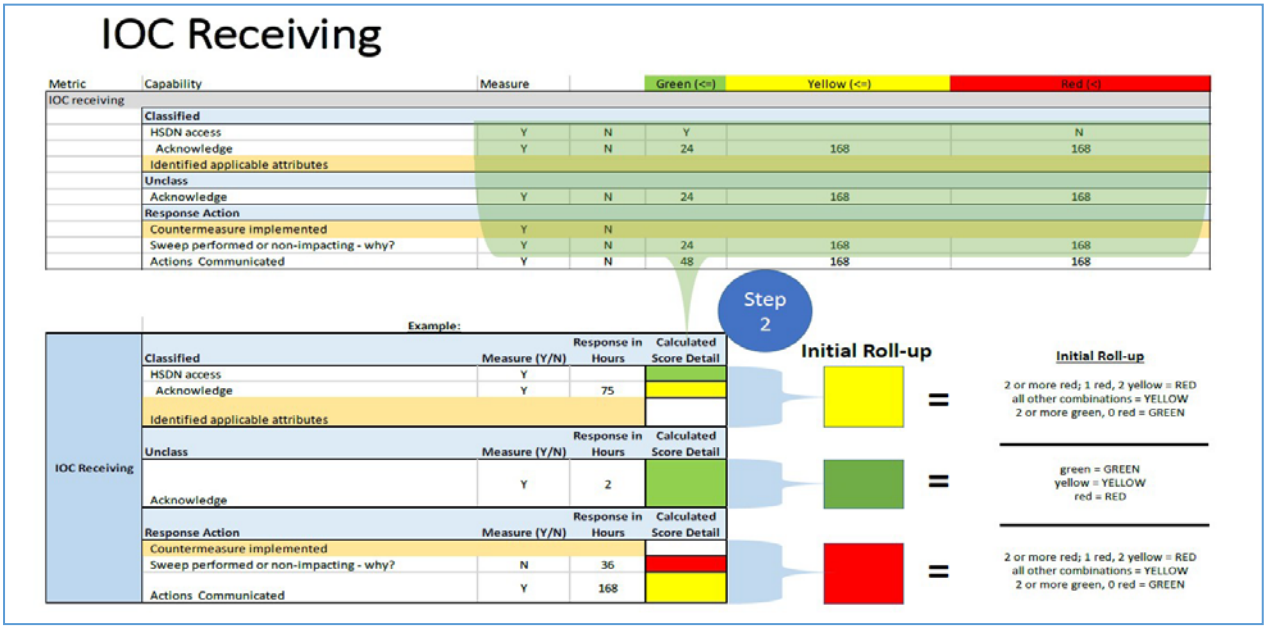


Figure 18: IOC Receiving Step 2

Figure 19: Calculation of the Final Score

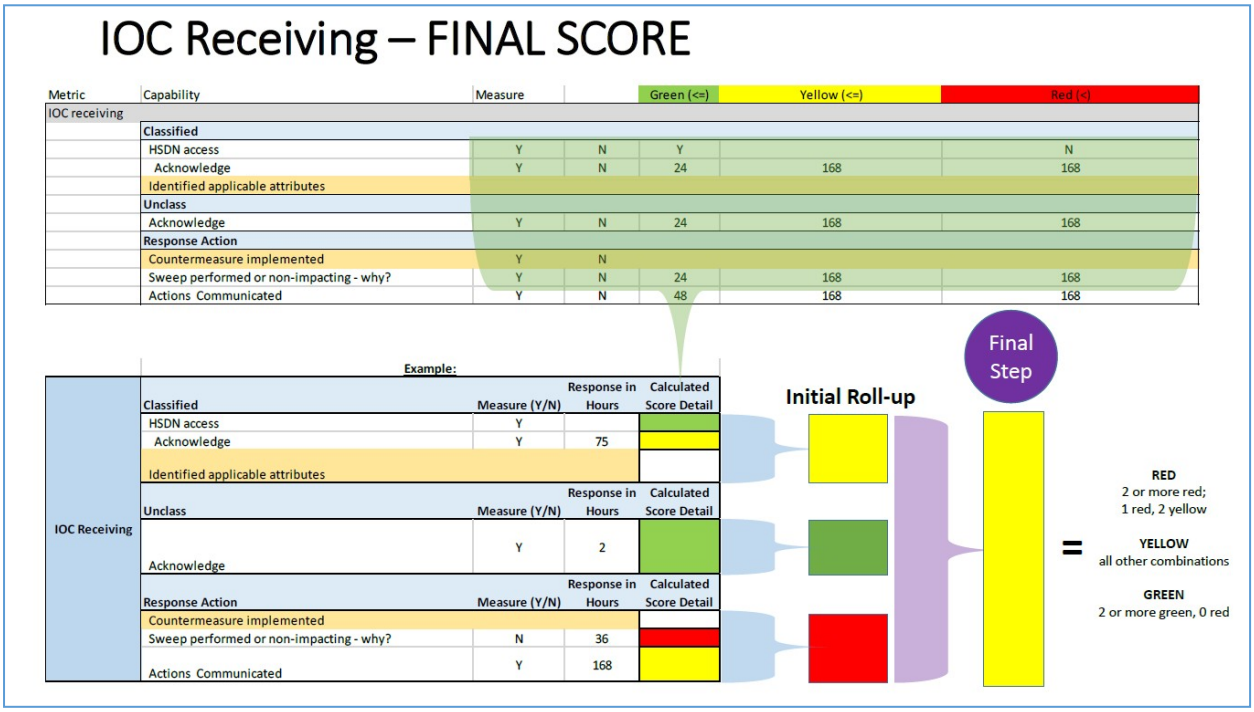


Figure 19: IOC Receiving, Final Score

Appendix H. INTRUSION DEFENSE CHAIN SCORING CRITERIA

Figure 20: The Calculated Score Detail.

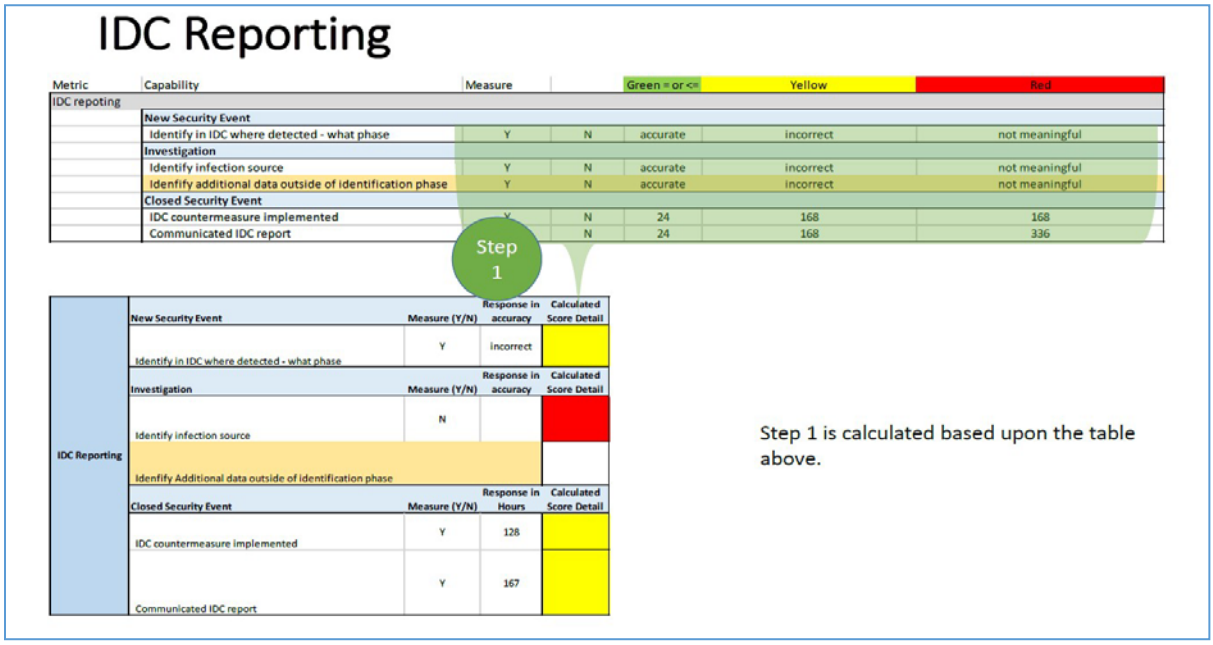


Figure 20: IDC Reporting Step 1

Figure 21: The Initial Rollup.

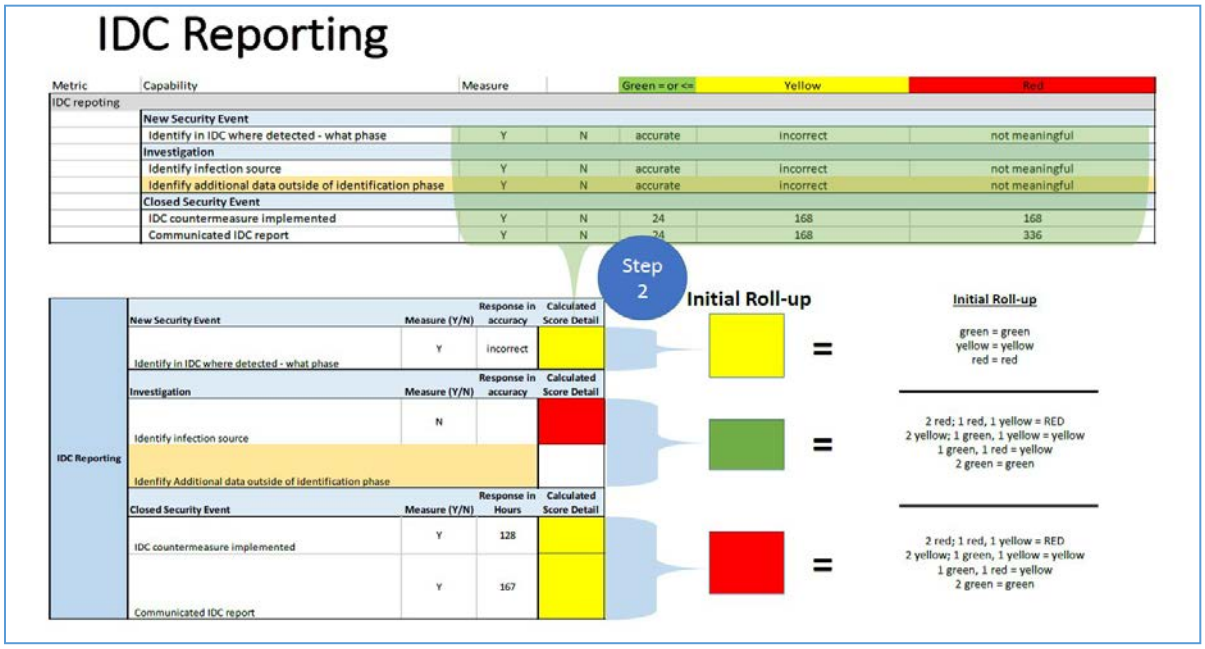


Figure 21: IDC Reporting Step 2

Figure 22: Calculation of the Final Score

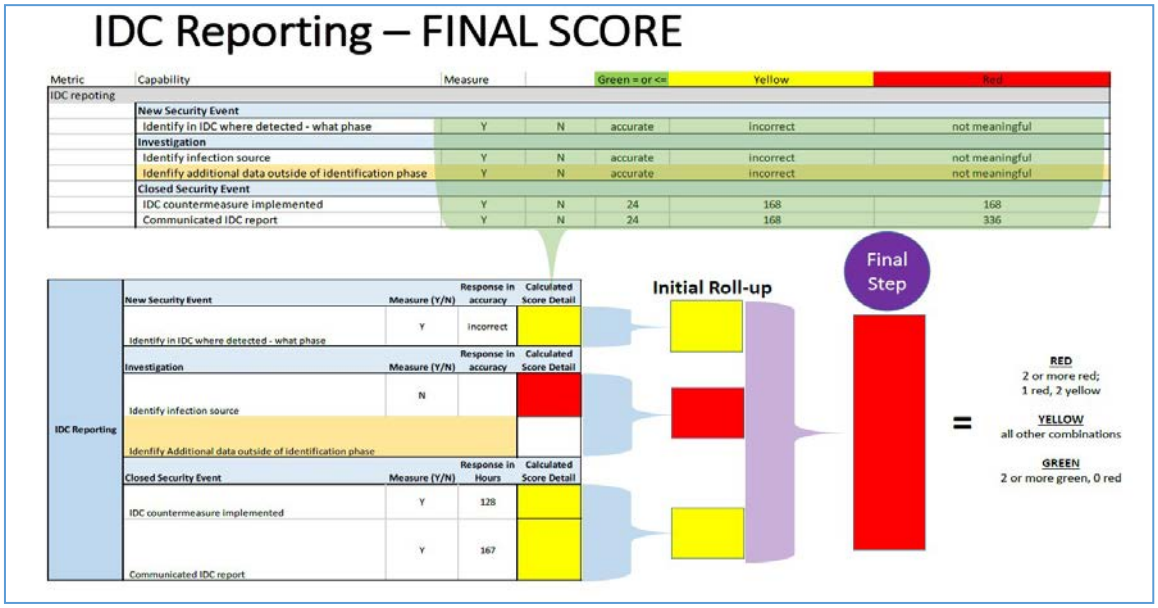


Figure 22: IDC Reporting, Final Score

Appendix I. DHS NIST RMF WORKFLOW

Figure 23 shows the DHS NIST RMF workflow. The most recent version of the workflow is located on the IACS Portal.

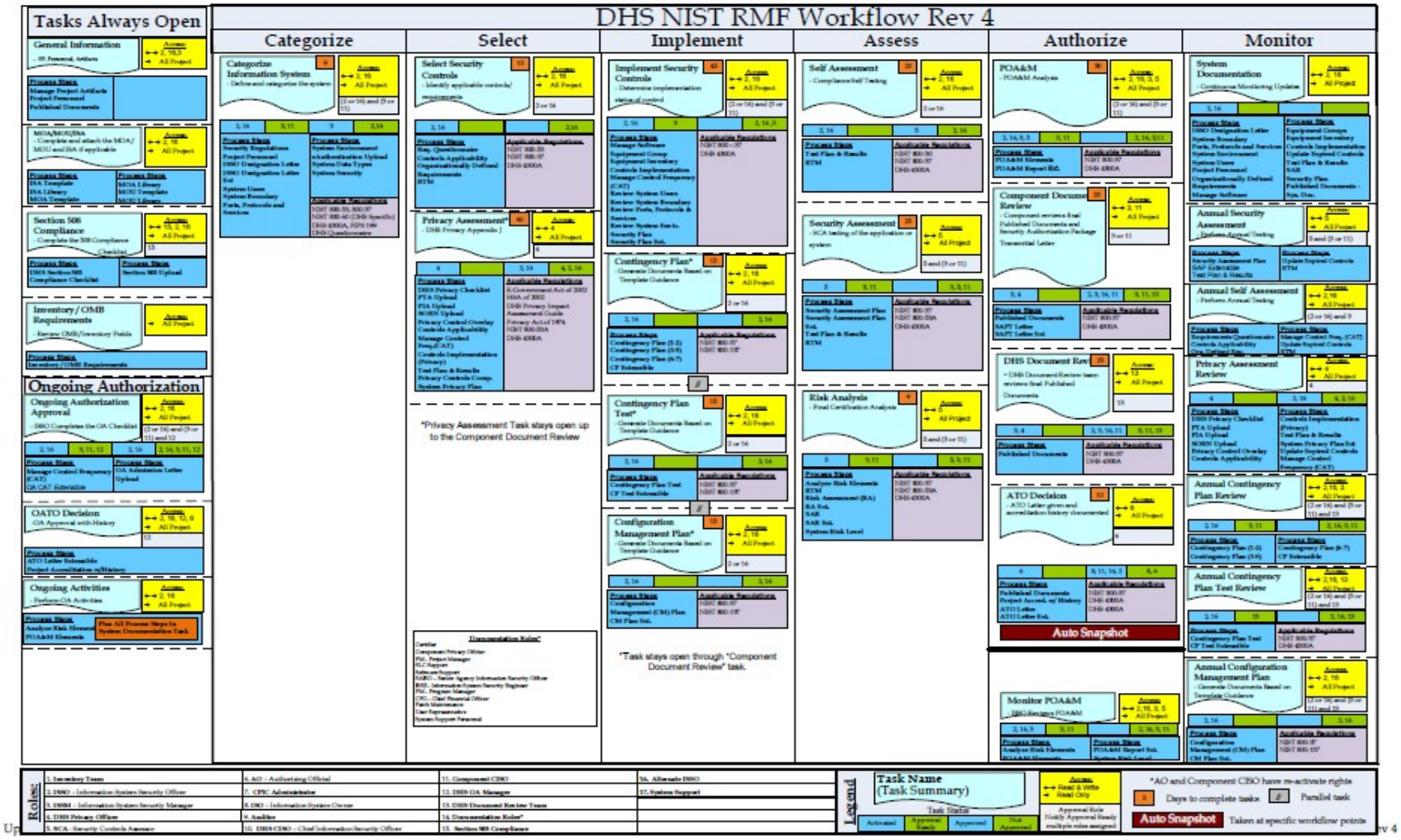


Figure 23: DHS NIST RMF Workflow

Appendix J. AVAILABLE CONFIGURATION AUDIT FILES

Figure 13 shows a short list of available configuration audit files. An official list of scored operating systems (OS) and versions is maintained on FISMA SharePoint and CMWG SharePoint.

Table 41: Available Configuration Audit Files

OS/Version	Authority	Modified Date	Checklist Name (Version)	Resources	On CMWG SharePoint
HP HP-UX 11.31	DISA	12/12/16	HP-UX 11.31 STIG (Ver. 1, Rel. 12)	SCAP 1.1 Content - HP-UX 11.31 STIGS Benchmark, Ver. 1, Rel. 13	NO
IBM AIX 5.3	DISA	05/28/14	AIX 5.3 STIG (Ver. 1, Rel. 2)	SCAP 1.1 Content - AIX 5.3 STIG Benchmark, Ver. 1, Rel. 2	NO
IBM AIX 6.1	DISA	12/12/16	AIX 6.1 STIG (Ver. 1, Rel. 9)	SCAP 1.1 Content - AIX 6.1 STIG Benchmark, Ver. 1, Rel. 9	NO
Microsoft Windows 7	DISA	12/12/16	Microsoft Windows 7 (Ver. 1, Rel. 24)	SCAP 1.1 Content - Windows 7 STIG Benchmark Ver. 1, Rel. 30	YES
Microsoft Windows 8 x86 (32-bit)	DISA	12/12/16	Windows 8/8.1 STIG (Ver. 1, Rel. 15)	SCAP 1.1 Content - Windows 8 STIG Benchmark - Ver. 1, Rel. 16	YES
Microsoft Windows 8 x64 (64-bit)	DISA	12/12/16	Windows 8/8.1 STIG (Ver. 1, Rel. 15)	SCAP 1.1 Content - Windows 8 STIG Benchmark - Ver. 1, Rel. 16	YES
Microsoft Windows 8.1 (x64)	DISA	12/12/16	Windows 8/8.1 STIG (Ver. 1, Rel. 15)	SCAP 1.1 Content - Windows 8 STIG Benchmark - Ver. 1, Rel. 16	YES
Microsoft Windows 8.1 (x86)	DISA	12/12/16	Windows 8/8.1 STIG (Ver. 1, Rel. 15)	SCAP 1.1 Content - Windows 8 STIG Benchmark - Ver. 1, Rel. 16	YES
Microsoft Windows 10	DISA	12/23/16	Windows 10 STIG (Ver. 1, Rel. 7)	SCAP 1.1 Content - Windows 10 Benchmark Ver. 1, Rel. 4	YES
Microsoft Windows Server 2008	DISA	12/12/16	Windows Server 2008 STIG (Ver. 6, Rel. 34)	SCAP 1.1 Content - Windows 2008 DC STIG Benchmark - SCAP - Ver. 6, Rel. 36	YES
Microsoft Windows Server 2008 R2	DISA	12/12/16	Microsoft Windows 2008 R2 STIG (Ver. 1, Rel. 20)	Standalone XCCDF 1.1.4 - Windows 2008 R2 MS STIG - Ver. 1, Rel. 20	YES
Microsoft Windows Server 2012	DISA	06/02/15	Windows 2012 (Ver. 1, Rel. 4)	SCAP 1.1 Content - Windows 2012 MS STIG Benchmark Ver. 1, Rel. 4	YES
Red Hat Enterprise Linux 5	DISA	12/12/16	Red Hat 5 STIG (Ver. 1, Rel. 16)	SCAP 1.1 Content - Red Hat 5 STIG Benchmark, Ver. 1, Rel. 17	YES
Red Hat Enterprise Linux 6	DISA	12/12/16	Red Hat 6 STIG (Ver. 1, Rel. 13)	SCAP 1.1 Content - Red Hat 6 STIG Benchmark, Ver. 1, Rel. 13	YES

OS/Version	Authority	Modified Date	Checklist Name (Version)	Resources	On CMWG SharePoint
Sun Solaris 10 SPARC	DISA	12/12/16	Solaris 10 (Ver. 1, Rel. 16)	SCAP 1.1 Content - Solaris 10 SPARC STIG Benchmark, Ver. 1, Rel. 16	YES
Sun Solaris 10	DISA	12/12/16	Solaris 10 (Ver. 1, Rel. 16)	SCAP 1.1 Content - Solaris 10 x86 STIG Benchmark, Ver. 1, Rel. 16	YES
Sun Solaris 11	DISA	07/01/16	Solaris 11 STIG (Ver. 1, Rel. 8)	SCAP 1.1 Content - Solaris 11 x86 STIG Benchmark - Ver. 1, Rel. 2	YES

Appendix K. AUTHORITIES

The requirements for the FY-17 Performance Plan are derived from the following sources:

Public Law 113–283, "Federal Information Security Modernization Act of 2014 (P.L. 113-283)" https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

OMB Memo M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government" https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

OMB Memo M-14-03, "Enhancing the Security of Federal Information and Information Systems" https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

OMB Memo M-14-04, "Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf

OMB Memo M-16-03, "Fiscal Year 2015-2016 Guidance on Improving Federal Information Security and Privacy Management Practices", https://obamawhitehouse.archives.gov /default/files/omb/memoranda/2016/m-16-03.pdf

OMB Memo M-17-05, "Fiscal Year 2016-2017 Guidance on Improving Federal Information Security and Privacy Management Practices", https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-05.pdf

"FY 2017 CIO FISMA Metrics", https://www.dhs.gov/sites/default/files/publications/FY%202017%20CIO%20FISMA%20Metrics-%20508%20Compliant.pdf

Appendix L. ACRONYMS AND ABBREVIATIONS

The following acronyms and abbreviations are used in this document:

Acronym	Definition
ADSP	Author Domain Signing Practices
AO	Authorizing Official
ATO	Authority To Operate
AV	Anti-virus
BIA	Business Impact Assessment
CAP	Cross Agency Priority
CAT	Control Allocation Table
CCC	Common Control Catalog
CCE	Common Configuration Enumeration
CCR	Critical Control Review
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMWG	Continuous Monitoring Working Group
COAV	Component Outreach and Assist Visit
CP	Contingency Plan
CPE	Common Platform Enumeration
CPT	Contingency Plan Test
CR	Change Request
CSM	Configuration Settings Management
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
CWG	Compliance Working Group
CyberMM	Cybersecurity Maturity Model
D/A	Departments/Agencies
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DIAR	DHS Information Assurance Repository
DiD	Defense in Depth
DISA	Defense Information Systems Agency

Acronym	Definition
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication Reporting & Conformance
DR	Document Review
EA	Enterprise Architecture
eGRC	Enterprise Governance, Risk, and Compliance
EIS	External Information System
ELA	Enterprise License Agreement
EMET	Microsoft Enhance Mitigation Experience Toolkit
EOC	Enterprise Operations Center
ePO	McAfee ePolicy Orchestrator
FCM	FISMA Compliance & Metrics
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FIPS Pub	Federal Information Processing Standards Publication
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
HQ	Headquarters
HSPD-12	Homeland Security Presidential Directive 12
HVA	High Value Asset
HW	Hardware
HWAM	Hardware Asset Management
IA	Information Assurance
IACS	Information Assurance Compliance System
ICAM PMO	Identity Credential and Access Management Program Management Office
ID	Identifier
ImD	Impact by Device
ImS	Impact by System
IMT	Inventory Management Team

Acronym	Definition
IOS	Internetwork Operating System
IP	Internet Protocol
IPREV	IP Reverse
IPT	Integrated Project Teams
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISVM	Information Security Vulnerability Management
IT	Information Technology
ITSO	Information Technology Services Office
JCMWG	Joint Continuous Monitoring Working Group
JCPMWG	Joint Cybersecurity Performance Metrics Working Group
LOE	Level of Effort
MAJ	Major Application
MES	Mission Essential System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAC	Network Access Control
NCAT	National Cybersecurity Assessment Technical Service
NFR	National Financial Record
NII	Not In Inventory
NIST	National Institute of Standards & Technology
NIST SP	NIST Special Publication
NPPD	National Protection and Program Directorate
NSI	National Security Information
NSS	National Security System
NVD	National Vulnerability Database
OA	Ongoing Authorization
OCIO	Office of the Chief Information Officer
OCISO	Office of Chief Information Security Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
ORMB	Operational Risk Management Board
OS	Operating System

Acronym	Definition
PCII	Protected Critical Infrastructure Information
PIA	Privacy Impact Assessment
PHI	Protected Health Information
PII	Personally Identifiable Information
PIV	Personal Identification Verification
POA&M	Plan Of Action & Milestones
POC	Point of Contact
PRIV	Privacy Office
PTA	Privacy Threshold Analysis
RMD	Risk Management Division
RMF	Risk Management Framework
RTM	Requirements Traceability Matrix
SA	Security Authorization
SAR	Security Assessment Report
SBU	Sensitive But Unclassified
SCAP	Security Content Automation Protocol
SLA	Service Level Agreement
SME	Subject Matter Expert
SOC	Security Operations Center
SORN	System Of Records Notice
SP	Security Plan
SPII	Sensitive Personally Identifiable Information
SSI	Sensitive Security Information
SSO	Single Sign On
SSP	System Security Plan
SAP	Security Assessment Plan
SW	Software
SWAM	Software Asset Management
TBD	To Be Determined
TIC	Trusted Internet Connection
TRAL	Trigger Accountability Log
TRM	Technical Reference Model
URL	Uniform Resource Locator
VAT	Vulnerability Assessment Team
VBR	Vouch by Reference

Acronym	Definition
VOIP	Voice over IP
VULN	Vulnerability Management