Privacy Impact Assessment
for the

Continuous Monitoring as a Service (CMaaS)

DHS/ALL/PIA-082

February 12, 2020

Contact Point
Luis Coronado
Deputy Chief Information Security Officer
Office of the Chief Information Security Office
(202) 447-5865

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), Chief Information Security Office (CISO) is leading the DHS enterprise-wide deployment of Continuous Diagnostics and Mitigation (CDM) tools under the Continuous Monitoring as a Service (CMaaS) Program to support the agency-specific efforts to implement adequate, risk-based, and cost-effective cybersecurity across DHS. CMaaS provides continuous monitoring, diagnostics, and mitigation capabilities designed to strengthen the security posture of DHS and its Components, systems, and networks through the establishment of a suite of functionalities that enable network administrators to know the state of their respective networks at any given time. CMaaS further informs Chief Information Officers (CIO) and Chief Information Security Officers (CISO) on the relative risks of cybersecurity threats, and makes it possible for Department personnel to identify, prioritize, and mitigate vulnerabilities. This Privacy Impact Assessment (PIA) is being conducted to cover the first two phases of the program (Asset Management and Identity and Access Management) and addresses the privacy risks associated with the deployment and operation of the CDM Agency Dashboard.

Overview

The Department of Homeland Security (DHS) is in the process of implementing the Continuous Monitoring as a Service (CMaaS) Program, which includes tools, sensors, and integration support services that support the planning, provisioning, configuration, operation, and management of tools, sensors, dashboards, and data feeds, to facilitate Continuous Diagnostics and Mitigation (CDM) governance.[1] The overarching CDM program's focus is to meet the requirements of Executive Order (E.O.) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,[2] which outlines a series of actions to enhance cybersecurity across federal agencies and reinforces the Federal Information Security Modernization Act (FISMA) of 2014[3] by holding agency heads accountable for managing cybersecurity risks. The CDM effort extends across the Federal Government, to include the DHS enterprise, and requires stakeholder and program management, measurement of successful monitoring, and alignment of projected/budgeted costs in support of the program objectives.

CDM tools enable the Department to fulfill its own cybersecurity requirements and to view customized reports in a dashboard that alerts security personnel to their most critical cyber risks. These alerts enable the Department to efficiently allocate resources based on the severity of the identified risk. Summary information from the individual DHS dashboard[4] (Agency Dashboard)

[1] For more information about the Federal Government-wide CDM program, which is managed by the Cybersecurity and Infrastructure Security Agency (CISA), please *see* DHS/CISA/PIA-030 Continuous Diagnostics and Mitigation (CDM), *available at* https://www.dhs.gov/privacy.

[2] *Available at* https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[3] 44 U.S.C. § 3551-3558.

[4] A dashboard provides a graphical overview, or summary, of the main information needed to manage security controls and maintain awareness of major network areas of concern.

feeds into the Federal Dashboard, managed by the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD), to inform and prioritize cyber risks across the Federal Government.

CDM Solution Architecture Overview

The goal of CDM is to enable federal civilian departments and agencies to expand their continuous diagnostic capabilities for securing their computer networks and systems by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts. Using commercial-off-the-shelf (COTS) tools, CDM makes agency summary system security data available to all departments and agencies via the CDM Federal Dashboard. This allows CISA CSD to support "the implementation of agency information security policies and practices for information systems"[5] consistent with its responsibilities as established by FISMA and policies and directives established by the Office of Management and Budget (OMB).[6, 7]

The CDM Solution Architecture is partitioned into Layers A, B, C, and D (See Figure 1).

- Layer A currently includes Asset Management (AM) and Identity and Access Management (IAM) capabilities, and provides the tools and sensors[8] used to capture the data required to deliver CDM capabilities.
- Layer B integrates data from the different tools and sensors and summarizes them into the Master Device Record (MDR) and Master User Record (MUR).
- Layers C and D provide data visualization of the CDM capabilities into the Agency Dashboard and CDM Federal Dashboard, respectively.

CMaaS consists of Layers A, B, and C, which are further explained in the below sections.

[5] 44 U.S.C. § 3553(b).
[6] Office of Management and Budget Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.
[7] Office of Management and Budget Memorandum M-16-04, The Cybersecurity Strategy and Implementation Plan (CSIP), https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.
[8] These tools and sensors identify risks or gaps in the agency's network protection or collect data from Department and Component networks in order to identify unusual or irregular network activity, such as an unsanctioned device being installed on an agency network or an adversary trying to exfiltrate agency data from the agency's network.

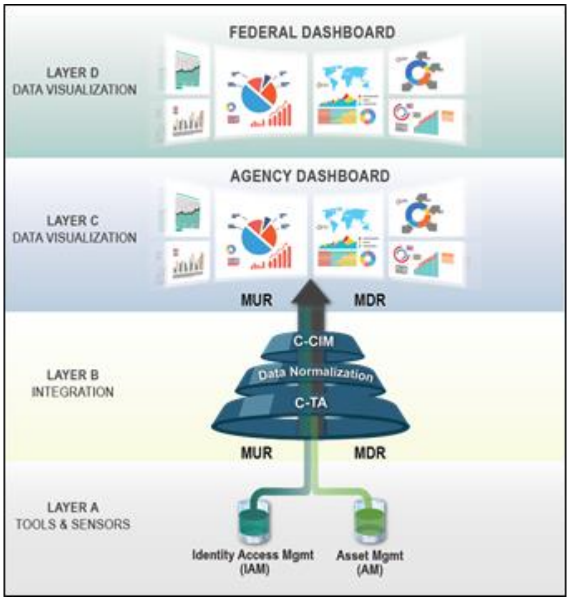

Figure 1 – Overall CDM Solution Architecture

CMaaS Solution Architecture Overview

CMaaS integrates enterprise-level Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), Vulnerability Management (VUL), Privileged Access Management (PRIVMGMT), and Credential Management (CREDMGMT) in the form of a standardized set of sensors, tools, and services throughout the Department. It allows the Department to realize on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service supporting a safe, secure, and resilient DHS network. The CMaaS solution also includes an Agency-level Dashboard that produces customized reports alerting network managers to the most critical cyber risks and provides a status on the Department's security posture. Agency installed sensors perform an automated search of the Department's endpoints[9] for known cyber risks. These scans are transmitted to the Agency-level Dashboard. An aggregation of the dashboard feeds is provided to the CMD Federal Dashboard to assist in security oversight and reporting. Since the CDM Federal Dashboard receives summary information, comprising predominantly of counts and no specifics, no personally identifiable information (PII) is shared.

Additionally, the implementation of CMaaS provides the following benefits:

- CMaaS deployed as a centralized service (through the existing on-premise cloud at DHS Data Centers) to all DHS IT assets residing in a federated infrastructure model.

[9] Endpoints are defined as workstations, laptops, and servers, and IP addressable network infrastructure elements.

- Tools and sensors implemented in a federated model providing Component-level service, capabilities, automation, dashboards, and limited customizations.
- Endpoint sensors on supported operating systems deployed throughout Component networks feeding near-real time data to CMaaS tools.
- Centralized management of the Component federated sensors, tools, automation, dashboards, and data.
- Department reporting capabilities and the ability to interface and interoperate with all Department and Component Security Operations, Network Operations, Ongoing Authorization, and Common Operating Picture programs and efforts.

CMaaS is organized by several phases (sometimes called CDM Capabilities). The first phase, Asset Management (AM), captures, manages, and controls information about "what is on the network." Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), and Vulnerability Management (VUL) are all managed and reported as part of this capability. The second CMaaS phase, Identity and Access Management (IAM), identifies, collects, and reports on "who is on the network." Specifically, the services identify and determine the users and their access authorization, authenticated permissions, and resource rights. These capabilities collectively cover the verification and validation of allowed user privileges, user owned credentials, user security behavior training, and appropriately granted resource access rights to users.

Asset Management (AM) – Phase 1

Asset Management comprises of four capabilities: Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), and Vulnerability Management (VUL). Asset Management focuses on endpoint integrity with a determination of what is on the network; what hardware, software, and systems are present; whether all systems are under configuration management, and vulnerability management (if any systems are at risk for compromise).

1. *Hardware Asset Management (HWAM)* provides visibility into the hardware devices operating on the network, new devices that connect to the network, authorization of devices, whether devices are managed, the prevention of malicious or compromised hardware from being installed on the system, and unauthorized hardware from being used for the unauthorized transfer of data.
2. *Software Asset Management (SWAM)* provides visibility into the software installed on devices/systems connected to the network by identifying all software actually present, whether software products are authorized, whether software products are up-to-date and patched, prevent or minimize compromised software, and identify software that are compromised, vulnerable, or targeted.

3. *Configuration Settings Management (CSM)* provides the ability to track and manage configuration settings of assets within the Department, mitigate attacks that require successful exploitation of default or poor configuration settings to compromise a device or system, prevent or minimize software from executing or processing potentially malicious or malformed input, stop or delay the compromise of devices due to misconfigurations, and stop or delay expansion or escalation via software vulnerabilities.

4. *Vulnerability Management (VUL)* provides visibility into known vulnerabilities present on the network associated with a specific set of software products and operating systems, to include IOS and firmware.

Asset Management does not involve any personally identifiable information (PII). Summary-level data, including device information, vulnerability details, software asset information, etc., from these four capabilities feed into the Agency Dashboard, and eventually the CDM Federal Dashboard, as depicted in Figure 2.

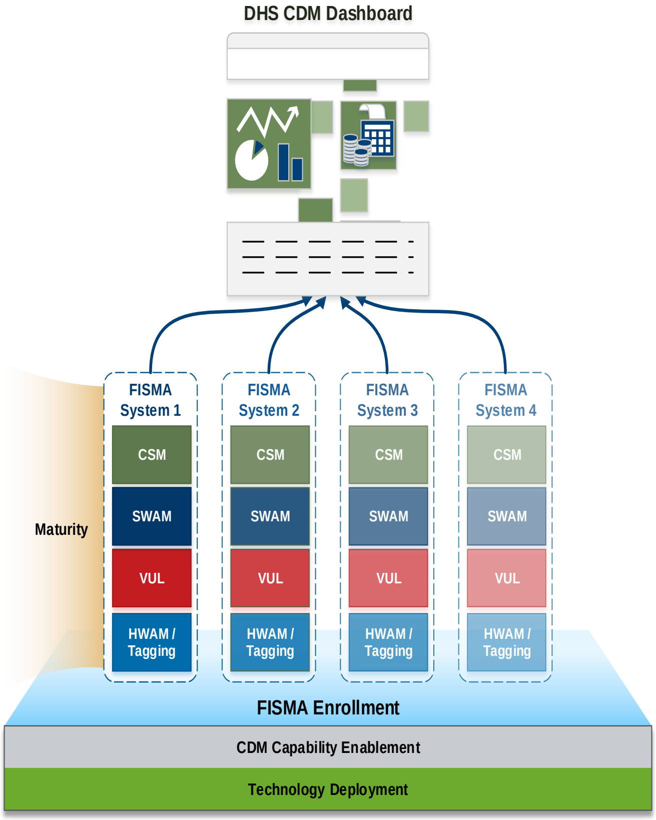

Figure 2 – Depicts the four capabilities of the Asset Management: HWAM, SWAM, CSM, VUL, and their reporting flow into the Agency Dashboard.

Identity and Access Management (IAM) – Phase 2

Identity and Access Management solutions identify, collect, and report on who is on the network. Specifically, the services identify and determine users and their access authorization, authenticated permissions, and resource rights. The capabilities collectively cover the verification and validation of allowed user privileges, user owned credentials, user security behavior training, and appropriately granted resource access rights to users.

IAM has been separated into two distinct efforts, Privileged Access Management (PRIVMGMT), which refers to the access a user has and Credential Management (CREDMGMT), which refers to the management of credentials a user uses to access the data and/or information on DHS and its component networks. To fulfill these objectives, IAM aggregates privileged and unprivileged management user PII from various authoritative sources to generate a Master User Record (MUR).[10] A MUR is maintained for every individual with access to the DHS network, and involves the management of that individual's attributes. The MUR data is broken down into five distinct categories: USER, Access Control Management (TRUST), Credentials and Authentication Management (CRED), Security-Related Behavior Management (BEHAVE), and Privilege (PRIV).

1. *USER*: Used as a construct that is used as an authoritative record of information for any particular person (or non-person) entity within DHS's purview. The USER entity serves as an anchor for the MUR which aggregates the other critical CMaaS attributes.

2. *Access Control Management (TRUST):* Used to validate a person's identity and the degree to which he or she has been vetted. The overall purpose of the TRUST area is to reduce the probability of loss in availability, integrity, and confidentiality of data by ensuring that only properly vetted users are given access to systems and credentials. This includes the requirement that the vetted trust level is properly monitored and renewed in a manner consistent with Department policy.

3. *Credentials and Authentication Management (CRED):* Binds a type of credential or authentication mechanism to an identity established in TRUST with a level of assurance and is used to grant access (physical and logical).

4. *Security-Related Behavior Management (BEHAVE):* Identifies that the individual has the proper knowledge and training for the roles in which the individual is assigned, and that training is current. This capability is defined in terms of how much or to what extent applicable training for individual roles has been provided and does not focus on user behavior.

[10] The MUR is a set of attributes or assertions about a user, with the user as the primary key (i.e., the "guaranteed unique" identifier in the database such as the EDIPI (electronic data interchange person identifier)).

5. *Privilege (PRIV):* The access rights granted to individuals (in terms of the privilege a user has to access areas within the system). PRIV data establishes the privileges associated with the credential and in turn the individual or service.

In order to configure a MUR about each individual user, CMaaS collects attributes from a number of authoritative data sources. It does so by leveraging the DHS Trusted Identity Exchange (TIE),[11] which is the DHS enterprise service that enables and manages the digital flow of identity, credential, and access-management data (attributes) for DHS personnel by establishing connections to various authoritative data sources and providing a secure, digital interface to other internal DHS consuming applications (e.g., CMaaS). Those data sources include the following:[12]

- Application Authentication System (AppAuth) for USER attributes;[13]
- Integrated Security Management System (ISMS) for TRUST attributes;[14]
- Identity Management System (IDMS) for CRED attributes;[15]
- Web Time & Attendance System (WebTA) for USER attributes;[16]
- Procurement Request Information System Management (PRISM) for USER attributes;[17]
- Human Capital Enterprise Integration Environment (EIE) for BEHAVE attributes;[18]

[11] For more information about the TIE, please *see* DHS/ALL/PIA-050 DHS Trusted Identity Exchange, available at https://www.dhs.gov/privacy.

[12] Generally, all attributes come from these authoritative source systems. However, there may be individual cases where one Component does not use one of these systems and instead provides the required attributes from another system. For example, some Transportation Security Administration (TSA) BEHAVE attributes come from the TSA Online Learning Center (OLC) because TSA does not use the enterprise Performance and Learning Management System (PALMS).

[13] AppAuth is a DHS enterprise system, which offers a single sign-on enterprise authentication service by providing a uniform authentication service, based on Microsoft's Active Directory (AD) services. For more information, please *see* DHS/ALL/PIA-060 Application Authentication System (AppAuth), *available at* https://www.dhs.gov/privacy.

[14] ISMS is a web-based case management tool designed to support the life cycle of DHS personnel security, administrative security, and classified visit management programs. For more information, please *see* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy.

[15] IDMS is the is the DHS enterprise-wide PIV issuance management system. For more information, please *see* DHS/ALL/PIA-014 Personal Identity Verification/Identity Management System (PIV/IDMS), *available at* https://www.dhs.gov/privacy.

[16] WebTA web-based time and attendance system developed to interface with the Department's payroll/personnel service provider, the National Finance Center (NFC). For more information, please *see* DHS/ALL/PIA-009 DHS Web Time and Attendance (WebTA) System, *available at* https://www.dhs.gov/privacy.

[17] PRISM is a contract writing management system that provides full procurement lifecycle support including all phases, from advanced acquisition planning, through contract closeout. Please *see* DHS/ALL/PIA-013 Procurement Request Information System Management (PRISM), *available at* https://www.dhs.gov/privacy.

[18] EIE serves as a consolidated authoritative source for human capital information across the Department, and it functions as a data broker among all enterprise-level HR systems at DHS. For more information, please *see* DHS/ALL/PIA-075 Workforce Analytics and Employee Records, *available at* https://www.dhs.gov/privacy.

- Performance and Learning Management System (PALMS) for BEHAVE attributes;[19]
- CyberArk for PRIV attributes;[20] and
- Privilege Access Manager (PAM) for PRIV attributes.[21]

The information from these data sources is filtered through the TIE to the Access Lifecycle Management (ALM) system,[22] where the MUR is maintained. ALM consolidates the information it receives from TIE, which is then aggregated to be presented at the Agency Dashboard. CMaaS is then able to compare that to the data captured by the tools and sensors (this is depicted as Layer A in Figure 1 above) to determine who is on the network and whether they should be or not. CDM requirements for Layer A mandate that the information displayed be updated at least every 72 hours. Information collected and stored as part of Layer B is retained for 90 days, after which it is automatically overwritten and/or purged from the system.

CMaaS Tools (Layer A)

The CMaaS Layer A is maintained by the individual Components. The Federal CDM Project Management Office (PMO) procured and installed an initial set of "baseline tools" to provide the capabilities defined under Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), and Vulnerability Management (VULN). However, Components have the flexibility to use alternates to the baseline tools, provided they perform the required integration activities. Although the tools and sensors deployed by Components may have additional capabilities, the CMaaS Program only requests and collects the specific data it requires to carry out its responsibilities. Below is a description of each of these baseline tools and the potential alternates Components employ. Below is a table of the baseline Asset Management tools and sensors and their alternatives, as well as the current Access and Identity Management tools and sensors. Appendix A will be updated as new tools or sensors are deployed for CMaaS.[23] This PIA will be updated if any new tools or sensors create new or additionally privacy risks.

[19] PALMS serves as an enterprise-wide DHS system, to automate the paper-based employee performance management process and consolidate multiple redundant e-training systems into a single integrated platform. For more information, please *see* DHS/ALL/049 Performance and Learning Management System (PALMS), *available at* https://www.dhs.gov/privacy.

[20] CyberArk is a COTS product used to enforce two-factor authentication for privileged users. To do this, CyberArk maintains a profile of each user and the computing assets the user is permitted to access.

[21] PAM, formally known as Xceedium as a Service (XCaaS), is an enterprise-wide software platform that provides secure access to DHS servers for authorized users and has tools for audit/compliance capabilities. The security mechanism handles all access and credential management across the DHS enterprise through linkages to privileged accounts.

[22] ALM is the technology and business process that manages the identities and access rights of DHS employees and contractors, ensuring that they only have access to approved systems and applications. For more information, please *see* DHS/ALL/PIA-058 Access Lifecycle Management, *available at* https://www.dhs.gov/privacy.

[23] A complete listing of the sensors/tools available for purchase by Components is available at the General Services Administration (GSA) CDM webpage: https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program.

Layer A & B – Baseline and Current Tools

Capability	Functionality	Baseline and Current Tools	Tool Alternates (Component Choice)
Hardware Asset Management (HWAM)	Managing “what is on the network?” requires the management and control of devices (HWAM), software (SWAM), security configuration settings (CSM), and software vulnerabilities (VUL).	Forescout - ForeScout appliances are used to conduct network discovery and hardware scans to provide Hardware Asset Management (HWAM) data for hardware assets (both physical and virtual) on the network. This Asset information is used to develop the Master Device Record.	Cisco ISE ServiceNow Tenable
Software Asset Management (SWAM)		McAfee Application Control (AC) – McAfee Application Control reduce risk from unauthorized applications to control endpoints, servers, and fixed devices. Using a dynamic trust model and innovative security features such as local and global reputation intelligence, real-time behavioral analytics, and auto-immunization of endpoints, this McAfee solution immediately thwarts advanced persistent threats (APT)—without requiring labor-intensive list management or signature updates.	Tanium App Locker Tenable
Configuration Settings Management (CSM)		McAfee Policy Auditor (PA) – McAfee Policy Auditor is an agent-based IT assessment solution that leverages the Security Content Automation Protocol (SCAP) to automate the processes required for internal and external IT and security audits.	Tenable
Vulnerability (VULN)		Retina - BeyondTrust Retina Network Security Scanner is an Enterprise vulnerability assessment solution that enables you to efficiently identify IT	Tenable Qualys

Capability	Functionality	Baseline and Current Tools	Tool Alternates (Component Choice)
		exposures and prioritize remediation enterprise-wide.	
Identity and Access Management	Managing "who is on the network?" through management and control of account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE).	CyberArk - CyberArk is a COTS product used to enforce two-factor authentication for privileged users.	
Identity and Access Management		PAM - PAM is an enterprise-wide software platform that provides secure access to DHS servers for authorized users and has tools for audit/compliance capabilities. The security mechanism handles all access and credential management across the DHS enterprise through linkages to privileged accounts.	Xceedium
Identity and Access Management		SailPoint - SailPoint Identity IQ identity management solution reduces the cost and complexity of both complying with regulations and delivering access to users. SailPoint enables you to efficiently manage digital identities, securely and confidently.	

Data Integration and Normalization (Layer B)

CMaaS employs a data integration process (Layer B) to compare the information collected from the tools and sensors to the MUR. The Data Integration Layer is implemented through the use of Splunk, which captures, indexes, and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards, and visualizations. This information, collected in the form of logs from the tools and sensors employed by DHS and its Components, is funneled to Splunk (through distributed Splunk infrastructure), which then analyzes the data to produce dashboards and visualization used by CMaaS users to meet CDM program objectives.

The current architecture has a dedicated Splunk instance for each Component to ensure access to data remains separated as appropriate. As CMaaS capabilities continue to expand, the Data Integration Layer is evolving from functioning as a data conduit between Layer A and Layer C, to providing more complex integration capabilities to include normalization of data between tools and sensors and creation of unique indexes for use by the Data Visualization Layer described below.

Data Visualization (Layer C)

The Data Visualization layer (the Agency Dashboard) is implemented using RSA Archer, which pulls the data from Splunk to generate reports. RSA Archer leverages the information it receives from Splunk and provides a compliance assessment and computes an Agency-Wide Adaptive Risk Enumeration (AWARE) score that provides a compliance and security posture for the agency and provides a graphical depiction of the agency's status.[24] These customized reports alert network managers to the most critical cyber risks and provides a status on the Department's security posture. From an Asset Management perspective, these reports include device information, vulnerability details, software asset information, etc. From an Identity and Access Management perspective, the dashboard reports contain information maintained in an individual's MUR. These reports also maintain object-level data reported from the Department and Component-installed tools and sensors which searches of the Department's endpoints for known cyber risks.

An aggregation of the Agency Dashboard feeds is provided to the CDM Federal Dashboard (Layer D) to assist in security oversight and reporting. Since the CDM Federal Dashboard receives summary information, comprising predominantly of counts and no specifics, no PII is shared.

Network Security Management and Data Protection Management - Future CMaaS Phases[25]

CMaaS Phase 3 involves the management of network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. This includes management of events (MNGEVT); operate, monitor, and improve (OMI); design and build-in security (DBS); boundary protection (BOUND); supply chain risk management (SCRM); and ongoing authorization. CMaaS Phase 4 involves the management of the protection of data through the capabilities: data discovery/classification (DISC); data protection (PROT); data loss prevention (DLP); data breach/spillage mitigation (MIT); and information rights management (IRM).

Access Control

In order to provide greater context to asset data as well as to facilitate role-based access (RBAC), the CMaaS solution entities are integrated with DHS enterprise and Component authentication technologies such as Active Directory (AD) and Privileged Account Manager

[24] AWARE provides an overall risk score for each endpoint, as well as an overall score for the entire agency. Risk scores are calculated using a number of variables, including asset criticality and the age of a vulnerability.

[25] The scope of this PIA does not include CDM Phase 3 and Phase 4 activities, as they are still in inception stages. This PIA will be updated to account for changes associated with these phases as appropriate.

(PAM). Role-based permission sets are created to allow Component personnel access for Component-specific endpoint product management and read-only access for specific products. Access and management of the Agency Dashboard is strictly controlled by the CMaaS System Owner through role-based access used to segment Component users for visibility to only their data. HQ DHS Staff and Component users requiring access to the CMaaS toolset must submit the request via their supervisor and the System Owner's representative in a Privileged Access Request (PAR)/Role Access Request (RAR) process as defined in the CMaaS Standard Operating Procedures (SOP). In addition to the DHS mandated training to protect PII that is required to be taken by all DHS personnel, the SOP outlines the tool specific training modules, the privileged user training, and the annual administrator training that the user must have completed in order to have access to the tools.

DHS CISO will continuously evaluate any potential risks to privacy and will update this PIA as appropriate to ensure the protection of data.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

CMaaS is consistent with and promotes carrying out numerous cybersecurity responsibilities. The statutory authority for CDM, and thus the functions of CMaaS, is as follows:

- Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551-3558) (FISMA), which directs the Secretary of DHS, in consultation with the Director of OMB, to administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems. FISMA further authorizes DHS to, upon request by an agency, deploy, operate, and maintain technologies to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities. This specifically authorizes the CDM program.
- Executive Order (E.O.) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*

Relevant policy directives that relate to CMaaS include:

- OMB Memorandum: Streamlining Authentication and Identity Management within the Federal Government (July 3, 2003);
- OMB Memorandum M-17-12: Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017);
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) – 12, Policy for a Common Identification Standard for Federal Employees and Contractors (February 3, 2011);

- OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems, (November 18, 2013);
- OMB Memorandum M-15-01, Guidance on Improving Federal Information Security and Privacy Management Practices (October 3, 2014); and
- OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (October 30, 2015).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

CMaaS acts as a broker between authoritative identity sources across the Department and the Agency Dashboard and CDM Federal Dashboard. All PII collected as a result of CMaaS tools and sensors is done so by the Component-level tools and sensors. The following SORNs are applicable to the maintenance of the MUR:

- OPM/GOVT-1 General Personnel Records;[26]
- DHS/ALL-003 Department of Homeland Security General Training Records;[27]
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS); [28]
- DHS/ALL-023 Department of Homeland Security Personnel Security Management;[29]
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System;[30] and
- DHS/ALL-037 E-Authentication Records.[31]

The GITAARS SORN covers the collection of general contact and other related information used to grant access to employees, contractors, and other individuals to the CMaaS solution and Agency Dashboard.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. A system security plan has been completed for CMaaS that supports the CDM

[26] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[27] DHS/All-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).
[28] DHS/ALL-004 General Information Technology Access Account Records Systems (GITAARS), 77 FR 70792 (November 27, 2012).
[29] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).
[30] DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).
[31] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).

efforts. The CMaaS Authority to Operate (ATO) is being reauthorized in conjunction with this PIA.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

CMaaS uses data from authoritative data sources that are covered by their own specific SORNs and retention schedules. However, for the reports that CMaaS does create, CMaaS follows the National Archives and Records Administration (NARA) disposition for IT Security, N01-0064-2008-0012: 817-3, 4a, and 5. The disposition states that these records are "Temporary." Section 5 below discusses the limited retention period for the data involved in CMaaS.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The Paperwork Reduction Act is not applicable. Information is not collected nor solicited directly from members of the public.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The Asset Management capability of CMaaS does not handle any PII. The below data elements are collected for the Identity and Access Management capability. This information is collected in ALM via the TIE to generate the Master User Record (MUR). Appendix B includes a table that corelates each attribute to a specific source system.

USER

MUR Data Element	Description
Unique Identifier	Used to uniquely identify a user within the MUR entries. Made up of Component Name and User ID (a number which is EDIPI) concatenated
AccountID	An attribute that captures a universally unique identifier that references a specific account on a physical or logical system.
Full Name	An attribute that allows for the entry of the Full name of a person at an agency.
First Name	An attribute that allows for the entry of the first name (i.e., Given Name) of a person at an agency.
Last Name	An attribute that allows for the entry of the last name (i.e., family name) with a generational qualifier, if required by agency policy, (e.g., Sr., Jr., III) of a person at an agency

MUR Data Element	Description
Middle Name	An attribute that captures the entry of a middle name (if available) of a person at an agency.
Email	An attribute that captures an electronic mailing address (email) for the identified user
Job Title	An attribute that captures the specification of a “job” or role title (e.g., Job Series, Functional Responsibilities) of a person as determined by an agency
Department	An attribute that captures a UID that identifies a specific organizational unit boundary
Component	An attribute that captures a UID that identifies a specific organizational unit boundary
User Status	An attribute that captures the last reported status of a user - the status shall be one and only one of the following values: • SEPARATED – User no longer actively exists within the agency (this is a permanent status with no anticipated return). • ACTIVE – User currently is active within the agency (i.e., employed or contracted). • SERVICE – Reserved for non-person entities, indicates the privileges/accounts associated with this entity are still in use. • INACTIVE – Reserved for temporary absences that are coordinated with the agency – Sabbatical, Detail, etc. • PENDING – Users who may not be active yet, are in the process of being on-boarded, vetted, trained, or otherwise prepared for duty.
User Type	An attribute that captures a type of user - the value of this attribute shall be one of the following: • GOVERNMENT • CONTRACTOR • NONPERSON (representing a non-person entity) • OTHER GOVT AGENCY (representing a “Detailee” or other assigned entity from another government agency that has been incorporated into the agency’s IT environment on a temporary basis).
Manager	An attribute that captures the individual’s manager/supervisor.

TRUST:

MUR Data Element	Description
Trust Identifier	An attribute that captures a universally unique identifier that references a specific TRUST instance.
Trust Status	An attribute that captures the current state of a TRUST authorization. The value of this attribute shall be one and only one of the following values: • PENDING • AUTHORIZED • SUSPENDED • EXPIRED • REVOKED

MUR Data Element	Description
Trust Type	An attribute that categorizes the type of screening/vetting required to establish a given instance of TRUST. The value of this attribute shall be one and only one of the following values: • INVESTIGATIVE – Investigative trust Levels require a certain amount of vetting (i.e., background investigations) prior to authorization and can often be represented in a hierarchy (e.g., Single Scope Background Investigation, National Agency Check with Inquiries (NACI), National Criminal History Check (NCHC)). • SUITABILITY – A process or mechanism to determine the fitness for employment or ability to grant access to resources. The scope of determining suitability may involve a review of personal conduct and/or other agency determined requirements that are in addition to other vetting processes (e.g., Entry on Duty Process – EOD). • ROB – Rules of Behavior Agreement that is a requirement prior to authorization. • NDA – Non-Disclosure Agreement that is a requirement prior to authorization. • FDA – Financial Disclosure Agreement (form) that must be completed prior to authorization. • AGENCYOTHER – Any unique agency processes used in the vetting/screening of users before establishing TRUST for a user within an agency.

CRED:

MUR Data Element	Description
CRED Identifier	An attribute that captures a universally unique identifier that references a specific CRED element.
CRED Type	An attribute that captures the class of a CRED element that has been inventoried by the system. Values for this attribute shall be one and only one of the following: • USERID PASSWORD • PIV CARD • BIOMETRIC • CAC CARD (Common Access Card - Department of Defense's version of a PIV CARD) • Level of Assurance 4 (LOA4) CREDENTIAL (other LOA4 Credential) • AGENCY OTHER
CRED Status	An attribute that captures the last reported status of a CRED element, which shall be one and only one of the following values: • PENDING • ISSUED • SUSPENDED • EXPIRED • REVOKED

BEHAVE:

MUR Data Element	Description
Training Identifier	An attribute that captures a universally unique identifier that references an appropriate security related BEHAVE element
Training Status	An attribute that describes the current status of the security-related BEHAVE element, valid values must be one of the following: • COMPLETED (BEHAVE is current, completed) • PENDING (a temporary status - BEHAVE has been assigned, is within grace period or otherwise in the process of being completed) • INCOMPLETE (BEHAVE has not been fully completed) • EXPIRED (BEHAVE has expired)
Training Type	An attribute that captures the class of a security-related BEHAVE element, which shall have one and only one of the following values: • CSAT (Cyber Security Awareness Training, as stipulated by FISMA metrics) • PHISHING (agency conducted phishing exercises, as stipulated by FISMA metrics) • ROLE TRAINING (role-based security training as defined by agency policy to fulfill requirements as stipulated by FISMA) • KNOWLEDGE (e.g., training or other event that increases skillset, knowledge building) • CERTIFICATION • AGENCY OTHER (e.g., other training not otherwise explicitly listed above including specialized purpose training requirements as determined by agency policy and/or routine general user training such as EOD security awareness training, rules of behavior training)

PRIV:

MUR Data Element	Description
PRIVID	An attribute that captures a unique identifier that references a specific PRIV instance.
PRIVType	An attribute that categorizes a PRIV instance, as determined by the type and scope of the elevated system(s) privileges bestowed to an account. This attribute shall be one of the following values: • SYSADMIN - System Administrator that has Administrative or Root level access on servers on the network. • SECADMIN - Security Administrator that has Administrative or Root level access on any target device on the network. • WINENTADMIN - Windows Enterprise Administrator has Authoritative Administrative access on all Active Directory Domain Controllers on the network (e.g., expansive control on federated domain controllers that are members of a forest, schema rights). • WINDOMAINADMIN - Windows Domain Administrator that has Administrative access on Active Directory Domain Controllers on the network. • WINWKSADMIN - Windows Workstation Administrator that has Administrative access on Active Directory-connected Workstations on the network. • MFADMIN - Main Frame Administrator that has Administrative access on Main Frame administrative functions on the network.

MUR Data Element	Description
	• ENTLDAPADMIN - Lightweight Directory Access Protocol (LDAP) server Administrator that has Administrative access on LDAP servers on the network. • MDMADMIN - Mobile Device Manager (MDM) Administrator that has Administrative access on MDM systems that control mobile devices on the network. • NETADMIN - Network Device Administrator that has Administrative access to network device administration control consoles (i.e., ISE, ACS, TACAS+, SolarWinds, JunOS Space) on the network. • AGENCYDEFINED - Synonymous to “Other”, this value allows agencies to capture the unique PRIVType categories that exist at an agency using the PRIVDescription attribute to add supplemental information (e.g., Database Administrator).
PRIVStatus	PRIVStatus – An attribute that captures the current state of a PRIV element or where it is in the issuance process, shall be one of the following values: • PENDING • ISSUED • SUSPENDED • EXPIRED • REVOKED
AccountID	An attribute that captures a universally unique identifier that references a specific account on a physical or logical system.
SystemBoundaryID	An attribute that captures a unique identifier that identifies a specific system boundary. This will be the unique key, name, or descriptor to identify a [FISMA] system for future reporting and reference.
Entitlement ID	An attribute that captures a unique identifier for a specific entitlement.
Entitlement Type	An attribute that captures the name [type] of entitlement that is inherent to the privilege that is associated with a higher-level privilege (e.g., FIREWALL, ROUTER, CORESWITCH).

Additionally, the tools and sensors employed by CMaaS collect device centric and user centric data (MUR centric) with the intent of assessing the security posture of agencies.

Finally, CMaaS collects user and login information from personnel who require access to the CMaaS capabilities.

2.2 What are the sources of the information and how is the information collected for the project?

CMaaS collections information from the following source systems to create and maintain the MUR: Application Authentication System (AppAuth), Integrated Security Management System (ISMS), Identity Management System (IDMS), Web Time & Attendance System (WebTA), Procurement Request Information System Management (PRISM), Human Capital Enterprise Integration Environment (EIE), Performance and Learning Management System (PALMS), and CyberArk or Privileged Access Manager (PAM).

Additionally, information is collected by the tools and sensors employed by the

Components to monitor their networks and systems.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. CDM does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

MUR attributes are collected by and maintained in ALM via the TIE from authoritative data sources. CMaaS is reliant on these authoritative data sources (source systems) to provide accurate and up-to-date data. By using the TIE, CMaaS ensures that it has information directly from these source systems, without any changes or manipulations to data integrity. CMaaS Program personnel also validate what is received and what is displayed on the Agency Dashboard, validating data using recurring and random checks.

Ultimately, Components are the authoritative source for their data and the information their tools and sensors collect and feed up to the Data Integration layer. Local component administrators can run queries and pull reports to verify that information being collected reflects what they know from their other sources.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that CMaaS maintains inaccurate information.

Mitigation: This risk is mitigated through several measures. First, information used to create the MUR is taken from authoritative source data. Second, CMaaS uses the TIE, a privacy-enhancing enterprise service that enables and manages the digital flow of identity, credential, and access-management data for DHS personnel, rather than any manual or less streamlined processes. Third, even if inaccurate data was used in CMaaS and determined an individual who is on the network should not be there, CMaaS itself does not take any action against that individual. CMaaS can just provide and alert to CMaaS administrators and appropriate personnel that a threat may exist.

Privacy Risk: There is a risk that CMaaS collects more information than is necessary.

Mitigation: This risk is mitigated. The CMaaS Program has determined the minimal amount necessary to complete it requirements to fulfill the CDM mandate. These data elements are generally administrative in nature and not considered sensitive PII. Furthermore, each Component's data is logically separated so that only those with an approved need-to-know are proved access. This is done through rule-based access controls.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

CMaaS is used to provide visibility into asset management, account management, and event/vulnerability management. The CMaaS solution further equips the Department with the ability to make sound, risk-based decisions to prioritize remediation of known vulnerabilities. Analysts at the Department-level will conduct trend analyses, and issue reports to assess the overall security posture of the Department; thereby assisting DHS and its Components to identify and mitigate vulnerabilities and reduce threat exposure. Likewise, CMaaS affords Components the opportunity to identify cybersecurity risks on an ongoing basis and mitigate the most significant issues first. Asset Management data is used to identify all the hardware components and associated software, configuration settings, and vulnerabilities in the network environment and develop mitigation plans to address risks. Identity and Access Management data is used to identify risky conditions to users, the access (including privileged access) that each user has, each user's training, and the user's credential levels.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. The Agency Dashboard and Splunk are configured to complete queries to identify and detect unexpected behavior based on hardware assets, software assets, configuration settings, and privilege/credential management. Queries are limited to data and information necessary to discover or locate a predictive pattern or an anomaly. Such a pattern or anomaly may include detecting whether installed software is performing an unauthorized action, whether a host is compliant with the configuration baseline, or whether a user is escalating his or her privileges to perform tasks outside of his or her normal responsibility

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. Each Component is responsible for the deployment of the tools and sensors it uses on its network. Additionally, each Component, through role-based access, has access to its own data on the CDM Agency Dashboard. Those with the appropriate need-to-know, to include DHS CISO personnel may require access to all of the component data on the dashboard.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized access to information maintained within CMaaS.

Mitigation: This risk is mitigated. Role-based access permission sets are created to allow Component personnel access for Component-specific endpoint product management and read-only access for CMaaS-specific products. While enterprise stakeholders (e.g., DHS CISO) have access to the Agency Dashboard across Component boundaries, role-based access is used to segment Component users for visibility to only their data. Access to the Agency Dashboard is strictly controlled and vetted by the system owner.

CMaaS is within the DHS network, follows FISMA guidelines, and uses FIPS-199 for its System Security Categorization. It is categorized as a system with an overall rating of High and implements security controls commensurate with the information it hosts. CMaaS has previously undergone the DHS certification and accreditation process that validates the implementation of those security controls, and is currently undergoing that process again.

Privacy Risk: There is a risk that information will be used inappropriately.

Mitigation: Role-based access permission sets are created to limit sharing of information across Component boundaries. Access to the Agency Dashboard is strictly controlled and vetted by the system owner. Prior to access being granted, individuals must complete dashboard training. Dashboard administrators and information assurance personnel are trained on DHS procedures for handling and safeguarding PII, in addition to DHS Mandatory Privacy Protecting Personal Information training, Cybersecurity Awareness training, and Rules of Behavior training. Furthermore, the system itself is not set up to take any actions independent of user action or manual intervention. CMaaS just provides the platform to consolidate and provide information to DHS personnel about the health of its networks, by providing alerts, reports, and ratings about potential network issues.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Users of Federal Government computer systems are provided with logon banners and sign user agreements that specifically notify them of the computer network monitoring. This PIA also serves as a notice to individuals that network traffic flow inbound and outbound is monitored and may be collected for computer Incident Response purposes.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All authorized users logging into their assigned agency IT systems and network are presented with an electronic notice or logon banner that notifies them the Federal Government system is being monitored. Users can elect not to use the Federal Government system or determine what information to transmit on the system.

CMaaS is not a general user system and is only intended as a tool for Cybersecurity staff across DHS.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that DHS personnel are unaware of the personal information CMaaS maintains or the network activity CMaaS tools and sensors collect.

Mitigation: This risk is not fully mitigated. Although users cannot be explicitly notified when their information is collected by CMaaS to create the MUR, all DHS personnel may reasonably expect that personal information may be used for administrative, managerial, and security functions at their agencies of employment. Further, CMaaS is not collecting any new data for the MUR; it is only pulling data from authoritative data sources which have already collected the information from those individuals. Those source systems may have other methods of notice, as described in their appropriate PIAs.

Although individuals cannot be explicitly notified when and what information is collected by CMaaS tools and sensors, the Department’s authorized network users receive notice by logon banners and user agreements that their communications or data transmissions are stored on the network, and that network traffic is subject to monitoring and disclosure for network security and other lawful government purposes.

Additionally, this PIA provides notice of CMaaS and the information it collects.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

CMaaS uses data from authoritative data sources that are covered by their own specific SORNs and retention schedules. Data from Layer A is refreshed every 72 hours, which ensures accurate data for the Master Device Record (MDR) and Master User Record (MUR) information. The Data Integration Layer, Layer B where Splunk is used, stores data collected from Layer A for a period of 90 days to help address conflicts with the data collected (the same retention applies to reports generated from both Splunk and RSA Archer). This duration is recommended by CISA and is not restrictive. Any component can choose to extend the retention period for longer to suit their operational needs, however the storage becomes the responsibility of the Component.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that data may be retained longer than necessary.

Mitigation: This risk is mitigated. CDM requirements mandate that the information displayed on the Agency Dashboard be updated at least every 72 hours. Information collected and stored as part of tools and sensor collection are retained for 90 days, at which time they are automatically overwritten and/or purged from the system.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

PII is not shared externally outside of DHS as part of normal agency operations. Although CMaaS shares data from the Agency Dashboard to the CDM Federal Dashboard (which even still, is maintained and operated by a DHS Component - CISA), that information is summary data and contains no PII.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

PII is not shared outside of DHS as part of normal agency operations.

6.3 Does the project place limitations on re-dissemination?

There are no limitations on re-dissemination of information produced by CMaaS because the reporting to the CDM Federal Dashboard does not contain PII.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

DHS does not share PII collected from CMaaS outside of the DHS. Both the Agency Dashboard and CDM Federal Dashboard maintain an accounting of what summary information is shared.

6.5 Privacy Impact Analysis: Related to Information Sharing

There are no privacy risks to external information sharing as no PII is shared. Any information that is shared outside of DHS to the CDM Federal Dashboard (event though it is maintained an operated by a DHS Component - CISA) does not contain PII.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

The data sources CMaaS uses for the MUR are the authoritative source systems from the Department or Components. None of this data is manipulated or changed. The procedures for correcting data shared to CMaaS lie with the source systems. The PIAs and SORNs applicable to that system provide additional information about the procedures to allow individuals access. There are no procedures to allow individuals to access their information in the Agency Dashboard or the information any tools or sensors collect. Access to the Agency Dashboard is strictly controlled and vetted by the system owner and is only intended as a tool for DHS cybersecurity personnel.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals do not have access to their information in CMaaS, and cannot correct it through CMaaS channels. Any inaccurate information should be corrected in the source system, similarly described above in Section 7.1.

7.3 How does the project notify individuals about the procedures for correcting their information?

Although individuals do not have access or the ability to correct their information in CMaaS, this PIA notifies individuals that they should reach back to the source systems and their procedures to correct information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not have the opportunity to correct inaccurate information in CMaaS.

Mitigation: This risk is not fully mitigated. Although it is unlikely that inaccurate or erroneous information is displayed or used in CMaaS as data has already been vetted from various authoritative sources to generate a Master User Record, individuals must go through those source systems to correct the information, rather than CMaaS. Additionally, if there was inaccurate information in the system, it would not affect the individually directly. For example, CMaaS currently does not have the ability to shut off a user's access to the network if it is determined that the individual does not have the appropriate BEHAVE attributes (e.g., a required training).

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

In addition to required privacy training, the system owner ensures proper handling of information through training awareness and accountability in conjunction with DHS CISO to ensure compliance and security of information. Access and management of the Agency Dashboard is strictly controlled by the CMaaS System Owner through role-based access used to segment Component users for visibility to only their data. Users requiring access to the CMaaS toolset must submit the request via their supervisor and the System Owner's representative in a Privileged Access Request (PAR)/Role Access Request (RAR) process as defined in the CMaaS SOP.

Further, the CMaaS ISSO maintains a list of users with privileged access to CMaaS. With role-based access controls in place for access control, personnel who leave DHS or a Component have their accounts either removed from Active Directory or inactivated/disabled. In either case, access to DHS CMaaS is restricted at that point.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Prior to access being granted to the Agency Dashboard, individuals must complete dashboard-specific training. Additionally, dashboard administrators and information assurance personnel are trained on DHS procedures for handling and safeguarding PII, in addition to DHS Mandatory Privacy Protecting Personal Information training, Cybersecurity Awareness training, and Rules of Behavior training. Further, the CMaaS SOP outlines tool specific training modules, privileged user training, and annual administrator training that the user must complete in order to have access to specific tools.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Users must obtain a favorable DHS suitability determination prior to being granted access to CMaaS. Users must also complete all mandatory privacy, security, and dashboard training. A role based-access request form must be completed and vetted first through the appropriate Component personnel (e.g., ISSO/ISSM) and then through the CMaaS System Owner for final approval. The process for granting user access is outlined in the CMaaS SOP.

Additionally, Component data is separated, and through the use of role based-access controls, only those individuals from that individual Component can see it, unless otherwise appropriate (e.g., a DHS CISO enterprise user or CMaaS administrator). Also, the Agency Dashboard tracks user activity (for a rolling 365-day period). If a user is not active within that period, the user may be marked as "inactive."

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Currently, the CMaaS Program does not share PII outside of DHS. Per DHS Sensitive Systems Policy Directive 4300A, the CMaaS Enterprise System Security Agreement (ESSA) documents all connections between Components and CMaaS. In the case PII is shared outside the Department or significant changes to access or new information sharing occurs, the CMaaS Program will work with the DHS Privacy Office to ensure all privacy requirements are fulfilled and risks mitigated, as appropriate.

Responsible Officials

Luis Coronado
Deputy Chief Information Security Officer
Office of the Chief Information Security Officer
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A

Layer A & B – Baseline Current and Alternate Tools

Capability	Functionality	Baseline and Current Tools	Tool Alternates (Component Choice)
Hardware Asset Management (HWAM)	Managing "what is on the network?" requires the management and control of devices (HWAM), software (SWAM), security configuration settings (CSM), and software vulnerabilities (VUL).	Forescout - ForeScout appliances are used to conduct network discovery and hardware scans to provide Hardware Asset Management (HWAM) data for hardware assets (both physical and virtual) on the network. This Asset information is used to develop the Master Device Record.	Cisco ISE ServiceNow Tenable
Software Asset Management (SWAM)		McAfee Application Control (AC) – McAfee Application Control reduce risk from unauthorized applications to control endpoints, servers, and fixed devices. Using a dynamic trust model and innovative security features such as local and global reputation intelligence, real-time behavioral analytics, and auto-immunization of endpoints, this McAfee solution immediately thwarts APTs—without requiring labor-intensive list management or signature updates.	Tanium App Locker Tenable
Configuration Settings Management (CSM)		McAfee Policy Auditor (PA) – McAfee Policy Auditor is an agent-based IT assessment solution that leverages the Security Content Automation Protocol (SCAP) to automate the processes required for internal and external IT and security audits.	Tenable Qualys
Vulnerability (VULN)		Retina - BeyondTrust Retina Network Security Scanner is an Enterprise vulnerability assessment	Tenable Qualys

Capability	Functionality	Baseline and Current Tools	Tool Alternates (Component Choice)
		solution that enables you to efficiently identify IT exposures and prioritize remediation enterprise-wide.	
Identity and Access Management	Managing "who is on the network?" through management and control of account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE).	CyberArk - CyberArk is a COTS product used to enforce two-factor authentication for privileged users.	
Identity and Access Management		PAM - PAM is an enterprise-wide software platform that provides secure access to DHS servers for authorized users and has tools for audit/compliance capabilities. The security mechanism handles all access and credential management across the DHS enterprise through linkages to privileged accounts.	Xceedium
Identity and Access Management		SailPoint - SailPoint Identity IQ identity management solution reduces the cost and complexity of both complying with regulations and delivering access to users. SailPoint enables you to efficiently manage digital identities, securely and confidently.	

Appendix B

External data sources contributing to MUR creation[32]

Source System	Existing Connected System[33]	Impacted MUR Functional Area	Specific MUR Attribute Needed
AppAuth	-	USER	Unique Identifier Full Name First Name Last Name Middle Name Email Job Title Department Manager Component User Status User Type AccountID
IDMS	ISMS	CRED	CRED Identifier CRED Type CRED Status
ISMS	-	TRUST	Trust Identifier Trust Status Trust Type
WebTA	EIE	USER	Manager (Federal Employees)
PRISM	ERA[34]	USER	Manager (COR & Contractor Employees)
PALMS, TSA OLC, FEMA FEIMS[35]	EIE	BEHAVE	Training Identifier Training Status Training Type

[32] This table only has external data sources that feed into the TIE. PRIV attributes are obtained from CyberArk and CA PAM that are CMaaS solution components, and not external systems.

[33] Some source systems have an additional connection before the information is passed through to the TIE.

[34] The Enterprise Reporting Application (ERA) is a minor application used to report procurement-related data and information from across the Department to the Office of the Chief Procurement Officer (OCPO) to support DHS-wide analysis and decision making.

[35] The Federal Emergency Management Agency (FEMA) Enterprise Identity Management System (FEIMS) is a system similar to IDMS used for authentication purposes.