Privacy Impact Assessment
for the

Continuous Diagnostics and Mitigation

DHS/NPPD/PIA-030

September 30, 2016

<u>Contact Point</u>
Andy Ozment
Assistant Secretary
Office of Cybersecurity & Communication (CS&C)
National Protection and Programs Directorate (NPPD)
(703) 235-5999

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

Abstract

The Department of Homeland Security (DHS) National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C) developed the Continuous Diagnostics and Mitigation (CDM) program to support Government-wide and agency-specific efforts to implement adequate, risk-based, and cost-effective cybersecurity. CDM provides continuous monitoring, diagnostics, and mitigation services designed to strengthen the security posture of participating federal civilian departments and agencies' systems and networks through the establishment of a suite of capabilities that enables network administrators to know the state of their respective networks at any given time, informs Chief Information Officers (CIO) and Chief Information Security Officers (CISO) on the relative risks of threats, and makes it possible for Government personnel to identify and mitigate vulnerabilities. This PIA is being conducted to cover Phase One, Two, and Three of the program and addresses privacy risks associated with CS&C's deployment and operation of the CDM Federal Dashboard.

Overview

While heightened Internet connectivity has transformed and improved public access to Government resources, it has also increased the extent and complexity of our shared cybersecurity risk. Cyber-attacks on Federal Government networks are growing more sophisticated, frequent, and dynamic. Accordingly, the Department of Homeland Security (DHS) National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C) established the Continuous Diagnostics and Mitigation (CDM) program[1] to fortify the cybersecurity of Federal Government networks and systems by acquiring integration services that provide continuous monitoring, diagnostics, and mitigation services to federal departments and agencies.

CS&C established an assisted acquisition vehicle including 17 blanket purchase agreements[2] (BPA) to allow it to centrally procure, operate, and maintain DHS-funded commercial-off-the-shelf (COTS) tools/sensors[3] and services that are deployed to participating

[1] Pub. L. No. 112-175, https://www.congress.gov/112/plaws/publ175/PLAW-112publ175.pdf.
[2] Found at, http://www.gsa.gov/cdm.
[3] Sensors identify risks or gaps in the agency's network protection or collect data from department and agency 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.

departments and agencies[4] as solutions to help manage hardware, software, configuration settings, and vulnerabilities at those departments and agencies.

CDM tools enable the department and agency to view customized reports in a dashboard that alerts security personnel to their worst and most critical cyber risks. Prioritized alerts enable departments and agencies to efficiently allocate resources based on the severity of the identified risk. Summary information from individual department and agency dashboards[5] feed into the Federal Dashboard, managed by CS&C, to inform and prioritize cyber risks across the Federal Government.

The Federal Dashboard managed by CS&C is composed of aggregate summary information from department and agency-level dashboards. No personally identifiable information (PII) is collected or maintained by the Federal Dashboard, but is instead collected and maintained by the individual departments' and agencies' implementation of CDM. CS&C does not have access to or control over the information collected and maintained at the respective departments and agencies. Each participating agency is responsible for assessing the collection, use, dissemination, and maintenance of information for their respective systems. The Federal Dashboard does not target the collection or generation of specific information about individuals. Data provided to the Federal Dashboard is not used to identify specific individuals, nor are records searchable by information that could be considered PII.

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 COTS tools, CDM makes agency summary system security data available to all departments and agencies via the CDM Federal Dashboard. This allows CS&C to support "the implementation of agency information security policies and practices for information systems"[6] consistent with its responsibilities as established by the *Federal Information Security Modernization Act of 2014*[7] and policies and directives established by the Office of Management and Budget (OMB).[8, 9]

[4] Office of Management and Budget Memorandum 15-01, FY 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf.
[5] 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.
[6] 44 U.S.C. § 3553(b).
[7] 44 U.S.C. §§ 3551-3558.
[8] Office of Management and Budget Memorandum 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.
[9] Office of Management and Budget Memorandum 16-04, *The Cybersecurity Strategy and Implementation Plan (CSIP)*, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

At a high level, the DHS CDM Program consists of three activities:

- Acquisition: Acquiring CDM sensors, services, and dashboards for participating departments and agencies.
- Implementation: Deployment of CDM sensors, services, and dashboards at participating departments and agencies.
- Operations: Operation of the sensors, as well as management of the CDM Federal Dashboard to identify, prioritize, and inform mitigation and oversight of systemic cybersecurity risks.

This PIA is being conducted to cover the first three phases (listed below) of the program and address privacy risks associated with CS&C’s deployment and operation of the CDM Federal Dashboard. These phases, which build upon each other, will enable departments and agencies to identify and then manage their network assets; identify and manage their users’ accounts; strengthen their boundary controls; and address and better manage their system security lifecycle, incidents, and operations. Departments and agencies continue to be responsible for their systems and the protection of the information on their respective systems. Once CDM is fully implemented, it is expected that departments and agencies will be in a continuously improving position to make risk-based decisions regarding the security posture of their networks.

CDM Phase One – Endpoint Integrity

During CDM Phase One, DHS coordinated the central management of the procurement, operations, and maintenance of COTS diagnostic sensors deployed to participating departments and agencies to help manage hardware, software, asset configuration settings, and vulnerabilities.

- Hardware Asset Management (HWAM): Visibility into the hardware devices operating on the network, new devices that connect to the network, authorization of the device, whether devices are managed, the prevention of malicious or compromised hardware from being installed on the system, and unauthorized hardware from being used for data exfiltration.
- Software Asset Management (SWAM): 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.

- Configuration Settings Management (CSM): Ability to track and manage configuration settings of assets within an organization; 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.

- Vulnerability Management (VULN): Visibility into the known vulnerabilities present on their networks associated with a specific set of software products and operating systems; to include IOS and firmware.

CS&C manages a Federal Dashboard that is fed with aggregate summary information from department and agency-level dashboards including:

- Hardware Inventory: Identifies hardware on networks by type, whether it is authorized or not, and whether it is managed or not.

- Software Inventory: Identifies software on networks by type, whether it is authorized or not, and whether it is managed or not.

- Configuration Settings: Identifies system platforms (hardware and software) that may or may not be configured according to agency-approved standards.

- Vulnerability Data: Identifies vulnerabilities on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.

CDM Phase Two - Least Privilege and Infrastructure Integrity

CDM Phase Two, which has been partially implemented as of the publishing of this PIA, involves the procurement and operations of monitoring equipment, diagnostic sensors, and dashboards that will provide risk scoring capabilities, to improve situational awareness at department and agency levels regarding people-based accounts services, leveraging the following capabilities:

- 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 that is consistent with department and agency policy.

- Security-Related Behavior Management (BEHAVE): Identifies that the individual has the proper knowledge and training for the roles to which he or she is assigned and that the training remains current. Note that this capability is strictly defined in terms of how much or to what extent applicable training for the individual's roles has been provided, and is not focused in a general manner on user behavior.
- Privileges (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.
- 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).

The CDM Phase Two solution will require the development and maintenance of a Master User Record (MUR)[10] for every person with access to the participating agency network, as well as management of attributes[11] associated with a CDM object. The MUR will reside within the confines of the associated agency system. Departments and agencies are responsible for their respective systems and the protection of the information on them.

Some PII may be collected by departments and agencies using Phase Two tools; however, no PII is returned to CS&C. Only high level summary data from each participating department and agency will be provided to the CS&C-managed Federal Dashboard. For example, Phase Two enables departments and agencies to manage access to accounts by ensuring that credentials and privileges are properly created and maintained, and that appropriate security training is occurring. At the agency level, Phase Two tools will collect information pertaining to an individual's suitability[12] and validity dates, clearance levels and validity dates, and training levels and completion dates. Agencies already have access ot this data. Information regarding the content of the suitability or clearance levels, however, is not collected by the CDM tools or returned to CS&C.

Occasionally, there may be an agency that does not have an identity aggregate system[13] for summary data of a Phase Two tool. In those cases, the CDM solution may involve creating the aggregate system for the agency. CS&C expects this to be a rare occurrence. But were this to occur,

[10] A 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)).

[11] Attributes describe a set of labels, values, and hierarchies associated with dimensions of anything that is a CDM object (i.e., anything that can pass or fail a defect check in CDM).

[12] 5 CFR 731.

[13] Aggregate system refers to an identity governance platform that pulls information from a number of Active Directories and can then summarize that information to report status to the CDM Federal Dashboard.

the creation of the aggregate system could involve some handling of PII by CS&C contractors that are supporting departments and agencies in the creation of the aggregate system. However, CS&C contractors will not provide any PII collected or maintained by the agency they support to the CDM Federal Dashboard, and in turn to CS&C. On the rare occasion that PII may be handled during the implementation of the CDM solution, the data contained within each participating agency system must follow federal protection and encryption standards for data in transit and at rest.[14]

CDM Phase Three - Boundary Protection and Event Management

CDM Phase Three will build upon the structure provided by Phases One and Two. Phase Three focuses on establishing a more extensive and dynamic set of controls to: establish internal actions and behaviors to determine who is doing "what" on the agency network; enable the agency to prepare for and respond to cybersecurity events or incidents; ensure software/system quality is integrated into the agency network/infrastructure; and enable the agency to mitigate security incidents to prevent propagation throughout the agency network/infrastructure. The Phase Three solution encompasses the following capabilities: Manage Events, Design and Build in Security, and Operate, Monitor, and Improve.

To complete the information gathered in Phases One and Two, which generally focus on the agency's internal network controls, Phase Three also includes Boundary Protection (BOUND). BOUND consists of three parts: BOUND-E for the evaluation of the encryption controls for the internal network, BOUND-F for the evaluation of the interactions outside of the internal network, and BOUND-P to address Physical Access Control Systems.

The Manage Events functionality will allow departments and agencies to prepare for cybersecurity events/incidents,[15] gather appropriate data regarding the cybersecurity event from appropriate sources,[16] and identify cyber incidents through the analysis of data.[17] The tools are centered on the ongoing assessment of selected CDM Phase One, Two and Three policy attributes for CDM network/infrastructure components. This ongoing assessment requires automating the process to monitor, collect, and analyze policy changes, which will capture CDM actual and/or

[14] For more information on federal encryption standards, please reference the Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, at: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[15] Identifies the different types of CDM security indicators, which are based on Phase One, Phase Two, and Phase Three attributes.

[16] The source for events can vary significantly, to include external intelligence sources, automated software components, hardware appliances, real-time analysis techniques, network monitoring tools, and proxy components.

[17] Includes the steps necessary to perform the initial verification of the event, assess the real-time threat, determine short term action, correlate events, identify incidents, and notify the network manager for further investigation.

desired state change events. The aggregation and correlation of these change events will result in specific CDM incidents, which will need an appropriate mitigating response.

The Design and Build In Security functionality will allow departments and agencies to prevent exploitable vulnerabilities[18] from being effective in the software/system while in development or deployment. The purpose of this function is to provide departments and agencies with the ability to identify, control, and remove weaknesses/vulnerabilities from the software/system.

During system/software development, this process begins with identifying security requirements and enforcing the use of security safe design/coding techniques during the design of the system/software, which will limit the exploit of known vulnerabilities. During deployment, the CDM Phase Three tool will utilize runtime security policies to continuously monitor and analyze the operating system platform and applications for runtime attack surface area weaknesses/vulnerabilities. Based on the weakness/vulnerability found, the Phase Three tool will ensure that appropriate mitigating controls and countermeasures are selected, applied to address the potential exploit, and verify the efficacy of the solution to mitigate the weakness/vulnerability for the departments and agencies.

The CDM Operate, Monitor, and Improve capability is focused on the ongoing authorization of agency network/infrastructure components – to include audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing). This ongoing authorization requires automating the process to analyze the events leading to incident risk, and based on the incident analysis, to recommend policy improvements to the agency to mitigate future incident threat activity. This capability will enable departments and agencies to continuously measure existing policies in order to identify improvements or recommend new policies that will increase the agency's security posture and reduce future security risks. The CDM Phase Three tool provides the ability for departments and agencies to perform near real-time risk management and mitigation, which will reduce the dependency on the standard three-year system security re-authorization/certification to apply updated security controls and countermeasures.

CS&C is conducting this PIA, prior to the full implementation of Phase Two, to provide transparency into the overall CDM program. No PII is collected by the Phase One tools. For Phases Two and Three some PII may be collected by the tools; however, no PII is returned to CS&C. Only

[18] Exploitable vulnerabilities may include software/system design, coding errors, software/system designs that leave a large and complex attack surface that cannot be defended, and weaknesses that can only be exploited during system/software execution.

high level (aggregated) systems status summary data from each participating agency will be provided to the CS&C-managed Federal Dashboard. Departments and agencies are responsible for their systems and the protection of the information on their respective systems.

A complete listing of the sensors/tools available for purchase by departments and agencies are available at the GSA website on the product catalogue page.[19] The catalogue provides the product name, a brief description of the product, and a link to the product manufacturer's website for more information. As new CDM capabilities are added through each phase of deployment there are refinements possible in the requirements related to previously implemented capabilities. These refinements typically include additional relevant data that must be collected in one capability that is utilized in the processes related to another capability. As these new capabilities are added, CS&C will continue to assess any potential privacy risks and will update this PIA, as appropriate.

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?

CDM is consistent with and promotes carrying out these responsibilities. The statutory authority for CDM is as follows:

- Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551-3558) (FISMA) 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, with or without reimbursement. This specifically authorizes the CDM program.

Relevant policy directives that relate to CDM include, but are not limited to the following:

- OMB Memorandum: Streamlining Authentication and Identity Management within the Federal Government (July 3, 2003)[20];

[19] Please visit, http://www.gsa.gov/portal/content/215827.
[20] Found at, https://www.whitehouse.gov/sites/default/files/omb/inforeg/eauth.pdf.

- OMB Memorandum M-06-16: Protection of Sensitive Agency Information (June 23, 2006)[21];
- OMB Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)[22];
- 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). The CDM Program will support visibility into agency HSPD-12 implementation of PIV access systems[23];
- OMB Memorandum M-14-03, Enhancing the Security of Federal Information and information Systems, (November 18, 2013)[24];
- OMB Memorandum M-15-01, Guidance on Improving Federal Information Security and Privacy Management Practices (October 3, 2014)[25]; and
- OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (October 30, 2015).[26]

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

CDM acts as a broker between authoritative identity sources across the solution and the agency and Federal Dashboards. All PII collected as a result of CDM operations in support of departments and agencies is done so by the agencies themselves. Therefore, SORN coverage is provided by the department or agency that subscribes to CDM as a service, if needed. CS&C does not have access to, or control over, the information maintained at the agency.

The Privacy Act applies when PII may be used as an identifier for authorized users[27] that have been granted system administration access to the CDM solution (such as username or a Government-issued email address). The Department of Homeland Security systems of records

[21] Found at, https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-16.pdf.
[22] Found at, https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf.
[23] Found at, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf
[24] Found at, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.
[25] Found at, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf.
[26] Found at, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf
[27] The term "authorized users" in this document refers to authorized and trained federal employees, contractors, and other individuals that have been granted access to the National Cybersecurity Protection System, which provides the infrastructure for many of CS&C's activities, and its related components.

titled, DHS General Information Technology Access Account Records Systems (GITAARS), November 27, 2012, 77 Fed. Reg. 70792, covers the collection of general contact and other related information used to grant access to employees, contractors, and other individuals to the CDM solution.

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

Yes. CS&C has received a FISMA identification number and follows the DHS certification and accreditation requirements for the CDM Federal Dashboard. Compliance with these requirements included the development of a system security plan for the CDM Federal Dashboard. DHS system accreditations are generally valid for three years from the date of authorization. The CDM Federal Dashboard is expected to receive its security authorization in fall 2016.

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

The CDM Federal Dashboard will be hosted on CS&C's National Cybersecurity Protection System (NCPS) Mission Operating Environment (MOE). The NCPS records retention schedules were approved by NARA on January 12, 2015, (Records Schedule Number: DAA-0563-2013-0008)[28] and August 6, 2015, (Records Schedule Number: DAA-0563-2015-0008).[29]

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 does not apply. Information is not collected or solicited directly from the public, nor is it collected by soliciting the same questions from 10 or more individuals.

[28] The Records Schedule is available at: http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0008_sf115.pdf

[29] The Records Schedule is available at: https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2015-0008_sf115.pdf

Section 2.0 Characterization of the Information

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

CS&C manages a Federal Dashboard that is fed with aggregate summary information from department and agency-level dashboards. No PII is collected or maintained by the Federal Dashboard, but is instead collected and maintained by the individual departments' and agencies' local instance of CDM. CS&C does not have access to or control over the information collected and maintained at the respective departments and agencies. Each participating agency is responsible for assessing the collection, use, dissemination, and maintenance of information for their respective systems.

CDM does not target the collection or generation of specific information about individuals. CDM disseminates network related summary security information from agency systems to the CS&C-hosted Federal Dashboard. CDM receives information originally collected by other sources and does not collect or generate any original data. CDM aggregates agency data from numerous source systems within the departments and agencies in order to generate usable information and reports. PII is not collected by these tools or included in the systems status summary information available in the CDM Federal Dashboard. The data is not used to identify specific individuals, nor are records searchable by information that could be considered PII.

General contact information such as name, title, agency name, email address, phone numbers, and other business related information may be collected to grant access to employees, contractors, and other individuals to the CDM solution.

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

CS&C will receive high level (aggregated) system status summary data from each participating agency, which feeds into the CS&C-managed Federal Dashboard.

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. The CDM Federal Dashboard does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The CDM solution is the broker of information between the agency source systems and the agency and CDM Federal Dashboards. The responsibility for ensuring and maintaining accurate information lies with the agency source system. That summary data then feeds into the CDM Federal Dashboard. CS&C has no mechanism for validating the accuracy of the summary data received from the departments and agencies since it does not have access to, or control over the information in the agency source system. The CDM program provides tools and implementation services to the departments and agencies focused on the exercising of consistent practices designed to ensure information accuracy in reported data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: The CDM solution may collect more data than is necessary, and due to the nature of how the data is collected, some information may be inaccurate.

Mitigation: Information collected by the CDM Federal Dashboard will not contain PII. However, collection of summary data from source agency systems may contain PII if the process is not properly and adequately defined and implemented. This risk is mitigated through the CDM program's development of guidance for departments and agencies to ensure that processes are developed and implemented that prevent the transmission of PII from departments and agencies into the CDM Federal Dashboard. In the unlikely event that CS&C receives PII via the agency summary data that feeds into the Federal Dashboard, CS&C cybersecurity analysts will follow cybersecurity information handling guidelines that require a review of collected information that could be considered PII, and the instructions for deleting such information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The CDM solution is used to summarize information between authoritative agency systems, and the agency and CDM Federal Dashboards in order to provide visibility into asset management, account management, and event management, as well as to provide departments and agencies with decision support for prioritization of remediation of vulnerabilities.

Using the information that feeds into the CDM Federal Dashboard, CS&C cybersecurity analysts will conduct trends analyses, assess the overall security posture of the federal agency enterprise, and issue reports to assist departments and agencies in mitigating those threats and vulnerabilities.

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. Though the CDM Federal Dashboard does not include PII, and is not configured or used to complete queries based on PII, queries will be performed to detect unexpected behavior based on software assets, hardware assets, or 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 a privileged action that it is not supposed to, or allowed to do.

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

Yes, participating components access the CDM Federal Dashboard but have restricted permissions to ensure they can only access the information pertinent to their specific component.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the collection of summary data from source agency systems may contain PII, which could be misused for purposes other than to aggregate for the CDM Federal Dashboard.

Mitigation: Information collected by the CDM Federal Dashboard will not contain PII. Federal Dashboard administrators and information assurance personnel are trained on DHS procedures for handling and safeguarding PII. CS&C cybersecurity analysts, system administrators, and information assurance personnel receive training upon hire, and are required to take refresher training each year. CS&C maintains standard operating procedures (SOP) for the purpose of identifying sensitive information, and for the proper handling and minimization of PII, to provide guidance for the necessary procedures and to define the terms for specifically identified roles and responsibilities. This allows CS&C to ensure that information collected by the CDM Federal Dashboard will not contain PII.

Departments and agencies that subscribe to CDM are responsible for adhering to their agency-defined processes and training for protecting PII.

Section 4.0 Notice

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 computer systems are provided with logon banners and sign user agreements that specifically notify them of the computer network monitoring. This Privacy Impact Assessment also serves as a general notice to individuals that network traffic flowing to or from participating federal departments and agencies may be collected for computer security purposes.

The CDM program does not provide any additional notice for the CDM Federal Dashboard prior to collection of information because it does not collect information about individuals.

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 agency's IT systems are presented with an electronic notice or banner that notifies them that Government computer systems are monitored. These users can then decide if they wish to use the system or not, and decide what information they want to transmit over the Government system.

Once a user decides to communicate with an agency electronically, by accepting the banner notice (in most cases clicking "OK" to proceed), the network traffic is subject to the computer security efforts of CS&C, including in this case the CDM Federal Dashboard. This monitoring is in addition to any individual computer security programs the agency might have in place.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a minimal privacy risk that individuals may choose not to read the notice or banner provided, or be aware of the information collection for CDM and the CDM Federal Dashboard.

Mitigation: DHS provides a variety of notice mechanisms to authorized users of Government systems, both inside and outside the agency. In addition, each participating agency's website contains a privacy policy stating that the agency uses computer security programs to monitor network traffic. Authorized users inside the agency networks receive notice by the agency's use of logon banners and user agreements notifying agency personnel that their communications or data transmissions are stored on their agency's network, and that network traffic is subject to monitoring and disclosure for network security and other lawful Government purposes. The disclosures outlined in those notifications include the summary (aggregate) data that is fed to the CDM Federal Dashboard. However, the impact with regards to the Federal Dashboard remains minimal as it only contains aggregate information and not PII.

With respect to the CDM Federal Dashboard, individuals may also access publicly available cybersecurity related PIAs or visit the DHS Privacy website, which provides additional resources explaining the DHS cybersecurity mission and its supporting programs. Additionally, CS&C maintains consistency across its individual program web pages by routing all links associated with Privacy Policy directly to the DHS Privacy Policy web page, ensuring that there are no discrepancies in how data is handled within the Department.

Section 5.0 Data Retention by the project

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

The CDM Federal Dashboard is hosted on the NCPS MOE. The National Archives and Records Administration (NARA) approved a records retention schedule (Records Schedule Number: DAA-0563-2013-0008) for NCPS on January 12, 2015.[30] The NCPS records retention schedule is broken down into five broad capability areas and covers all fields and data collected by and maintained on NCPS, including the data collected by the CDM Federal Dashboard and any resulting reports and analysis. The NCPS records retention schedule covers all cyber threat information, and is not broken down by program. Generally, NPPD will destroy or delete cyber threat information when it is three years old or when it is no longer needed for agency business, whichever is later. A second NCPS records retention schedule (Records Schedule Number: DAA-0563-2015-0008) was approved by NARA on August 6, 2015[31] and covers the disposition of operational NCPS data that is inadvertently collected or captured by any or all NCPS capabilities and that are determined not to be related to known or suspected cyber threats or vulnerabilities. Information that is inadvertently collected or determined not to be related to known or suspected cyber threats or vulnerabilities will be destroyed or deleted immediately or when it is no longer needed for agency business (e.g., after the completion of analysis). Other exceptions include analysis, reports, and forensic files.

[30] The link to the approved NARA Record Schedule DAA-0563-2013-0008 is included here: http://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0008_sf115.pdf.

[31] The link to the approved NARA Record Schedule DAA-0563-2015-0008 is included here: https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2015-0008_sf115.pdf.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that PII may be inadvertently collected and retained beyond what is necessary to appropriately aggregate the summary information for the CDM Federal Dashboard.

Mitigation: CS&C will retain information obtained through the CDM Federal Dashboard for no longer than reasonably necessary to discover and delete the PII. A records retention schedule for NCPS (Record Schedule #DAA-0563-2013-0008 and updated with DAA-0563-2015-0008) was approved on January 12, 2015 and August 6, 2015, respectively.

Section 6.0 Information Sharing

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.

As part of its computer network security responsibilities, CS&C generates reports on topics including general computer network security trends; specific incidents; and anomalous or suspicious activity observed on federal networks. The identification of specific individuals or entities is not included in the reports. These reports are made available to DHS organizations, including the National Cybersecurity and Communications Integration Center (NCCIC) and other Federal Executive departments and agencies, through systems such as the US-CERT.gov secure website for their use in infrastructure protection and other computer network security related responsibilities.

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

CDM acts as a broker between authoritative identity sources across the solution and the agency and Federal Dashboards, but does not share this information. CS&C does not have access or control over the information maintained at the agency. Because CS&C does not maintain this information or retrieve the information by a personal identifier, a SORN is not required.

6.3 Does the project place limitations on re-dissemination?

There are no limits on the re-dissemination of reports generated from the summary information contained in the CDM Federal Dashboard.

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

Since the CDM solution does not put limits on re-dissemination of the information, there is no need to maintain a record of disclosures. The Privacy Act accounting of disclosures requirement does not apply in this circumstance given the Federal Dashboard does not contain PII or Privacy Act-covered data.

6.5 Privacy Impact Analysis: Related to Information Sharing

There are no privacy risks to external information sharing as no personally identifiable information is shared. Any information that could be considered PII is destroyed before sharing.

Section 7.0 Redress

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

There are no procedures to allow individuals to access their information in the CDM Federal Dashboard because the CDM Federal Dashboard does not contain information on individuals.

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

There are no procedures for individuals to correct information in the CDM Federal Dashboard because the CDM Federal Dashboard does not contain information on individuals.

An individual who serves as a point-of-contact for CDM at their agency can submit a written request to DHS/NPPD Freedom of Information Act (FOIA) Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380, to have his/her inaccurate or erroneous contact information corrected, if collected by CS&C. However, he or she may receive a more timely response by contacting GSA or DHS staff directly at cdm@gsa.gov or cdm.fnr@hq.dhs.gov respectively.

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

Procedures to allow individuals to correct inaccurate or erroneous information are the responsibility of the participating agency as the underlying source system owner.

7.4 Privacy Impact Analysis: Related to Redress

There are no redress procedures beyond those described above and afforded under the Privacy Act and FOIA. Redress procedures to allow the subject individual to correct inaccurate or erroneous information are the responsibility of the participating agency as the underlying source system owner.

There are no risks related to redress given there is no collection of PII in the Federal Dashboard. The risks of redress occur at the agency level and must be implemented by the agency that collets the underlying data

Section 8.0 Auditing and Accountability

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

By design, the Federal Dashboard does not collect PII and is the primary way in which CDM ensures information is used in accordance with the stated practices. Additionally, specific information handling SOPs to ensure awareness, accountability, and compliance of what information should and should not be shared, are circulated annually to the CS&C cybersecurity analysts. Memorandums of Agreement (MOA) (described in 8.4) also establish requirements and controls for the handling of information in a manner consistent with this PIA.

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

DHS provides the required privacy and security awareness training to all employees and contractors supporting the implementation of the CDM solution for agency customers, as well as to CDM Federal Dashboard system administrators and information assurance personnel, which equips them with information on safeguarding PII.

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

CS&C users must obtain a favorable DHS suitability determination prior to acquiring access to the CDM Federal Dashboard. In addition, CS&C maintains cybersecurity information handling guidelines for the proper handling and minimization of PII. The guidelines outline the necessary procedures and define the terms for specifically identified roles and responsibilities. These guidelines are provided to CS&C cybersecurity analysts, as well as system and network administrators so that they are aware of what information should and should not be shared.

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?

The MOAs developed between DHS and other departments and agencies are based on an approved template that has been fully coordinated through the program manager, system owner, and Office of the General Counsel. New uses of the information and new access to the system by organizations within and outside of DHS are similarly reviewed by various stakeholders, including integrated program teams with approval vetted through upper management. Such reviews include vetting by the NPPD Office of Privacy, in collaboration with the DHS Privacy Office, to ensure privacy controls are included and any other privacy equities are accounted for.

Responsible Officials

Andy Ozment
Assistant Secretary
Office of Cybersecurity & Communications
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

____

Jonathan Cantor
Acting Chief Privacy Officer
Department of Homeland Security