Privacy Impact Assessment Update
for the

Continuous Diagnostics and Mitigation (CDM)

DHS/CISA/PIA-030(a)

December 19, 2019

Contact Point
Kevin Cox
Program Manager, CDM PMO
Cybersecurity Division
Cybersecurity and Infrastructure Security Agency
(703) 235-3924

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

Abstract

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) 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 tools and services 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 security officials and 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 Update is being conducted to assess the privacy risks related to the CDM Shared Service Platform, which makes CDM capabilities available for use by non-Chief Financial Officer (CFO) Act agencies. The Shared Service Platform is provided to non-CFO Act agencies using a third-party contractor to CISA that connects the agency's network(s) to the platform. Additionally, this PIA Update examines the CDM Agency-Wide Adaptive Risk Enumeration (AWARE) capability. The CDM AWARE capability allows participating agencies to better assess and prioritize cybersecurity risks by assigning a risk score to agency vulnerabilities.

Overview

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) established the Continuous Diagnostics and Mitigation (CDM) program to bolster the cybersecurity posture of Federal Government systems and networks by deploying tools, dashboards, and integration services that provide continuous monitoring, diagnostics, and mitigation services to federal departments and agencies.

CDM tools enable departments and agencies to view customized reports in a dashboard that alerts security personnel to critical cyber risks and vulnerabilities. There are two types of dashboards under the CDM program; the Federal Dashboard and the Agency Dashboard.

CDM Federal Dashboard:

- Displays summary-level CDM data from participating agencies.
- Provides information to oversight groups and federal cybersecurity analysts including those within CISA, the Office of Management and Budget (OMB), Offices of Inspectors General, and related offices responsible for monitoring government-wide IT risk.
- Communicates to the CDM Agency Dashboards in order to transmit risk scoring parameters as necessary. For example, if CISA identifies a new threat, it could recommend

a change in the risk scoring to reflect the urgency of mitigation. In addition, an authorized query from the Federal Dashboard will enable analysts at the federal level to obtain supplemental information when executed.

- Communicates policies and security information for agency awareness, such as Binding Operational Directives, indicators of compromise, etc.

CDM Agency Dashboards:

- Obtains object-level data from agency sensors and other agency sources via the CDM integration layer.
- Provides actionable information for system owners, security leadership, and system administrators to prioritize actions to improve network security.
- Supports the monitoring of risk and facilitates identification and reduction of specific risks on specific objects.

The goal of the CDM program is to enable federal civilian departments and agencies to expand their continuous diagnostic capabilities for securing their computer systems and networks by increasing their network sensor capacity, automating sensor collections, and prioritizing alerts by level of risk to the department or agency. CDM significantly improves the security posture of federal networks by using inputs from CDM tools and sensors to compare "desired state" to "actual state" data, allowing officials at each agency to quickly identify, prioritize, and mitigate risks.

The summary system data available via the Federal Dashboard also allows CISA to support "the implementation of agency information security policies and practices for information systems"[1] consistent with its responsibilities as established by the *Federal Information Security Modernization Act of 2014*[2] and policies and directives established by OMB.[3]

Reason for the PIA Update

CISA is conducting this PIA Update to describe the addition of a private instance of shared services on a publicly available cloud service provider (CSP) to the CDM program. This shared service solution provides CDM capabilities to non-CFO Act Agencies[4] using a systems integrator

[1] 44 U.S.C. § 3553(b).
[2] 44 U.S.C. § 3551-3558.
[3] Office of Management and Budget Memorandum 19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements,* https://www.whitehouse.gov/wp-content/uploads/2018/10/M-19-02.pdf.
[4] The Chief Financial Officers Act of 1990 (Public Law 101-576) was enacted to bring more effective general and financial management practices to 23 federal departments and agencies, with the Department of Homeland Security becoming the 24th upon its creation in 2001. A "non-CFO Act agency" is typically characterized as a small or independent agency with limited or shared resources. These resources include, but are not limited to, personnel,

(hereinafter "the integrator"), such as a third party contractor, that connects their network(s) to the cloud-based platform.

CDM Shared Service Platform

This CDM Shared Service Platform makes the below CDM capabilities[5] available to non-CFO Act agencies:

- Asset Management Capability (formerly Phase 1): Discovering what hardware and software are on the network, and whether or not they are authorized. "What is on the network?"
- Identity and Access Management Capability (formerly Phase 2): Discovering who is on the network, whether or not they are authorized to be there, and what privileges they have. "Who is on the network?"
- Network Security Management Capability (formerly Phase 3): Protecting the network through means such as firewalls and encryption. "What is happening on the network?"
- Data Protection Management Capability (formerly Phase 4): Protecting the data, whether at rest or in transit. "How is the data protected?"

The data collected by the tools and sensors within this shared service is provided to the agency through the integrator. The integrator has instituted controls to ensure that agency data is logically separated and segregated so that agencies subscribing to the shared service are only given access and user roles that are specific to their respective agency. The integrator will have access to the data collected by the tools through its Operations and Maintenance (O&M) responsibilities. Some of this data could include personally identifiable information (PII) or any other information that agency's data contains. However, the integrator will not use or share the agency data that is collected with CISA as specified in the Task Order Requirements for the shared service.

While CISA is funding the service, CISA does not receive or have access to any of the information that feeds into CDM at the agency level. As documented in the original iteration of the CDM PIA,[6] only agency summary data is fed into the CDM Federal Dashboard. Individual departments and agencies continue to be responsible for their respective systems and the protection of the information on those systems.

technology, IT systems, and/or budget.

[5] CDM capabilities have historically been divided into four phases. However, it became evident that the term "phase" implied a sequential ordering that was not correct. Therefore, the CDM Program now uses the term "capability."

[6] *See* DHS/CISA/ PIA-030 Continuous Diagnostics and Mitigation (CDM) (September 30, 2016), *available at* https://www.dhs.gov/privacy.

CDM Agency-Wide Adaptive Risk Enumeration (AWARE)

Additionally, this PIA Update examines the CDM AWARE capability. The CDM AWARE capability allows participating agencies to better assess and prioritize cybersecurity risks by assigning a risk score to agency vulnerabilities, meant to represent the risk of not mitigating a particular vulnerability.

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. AWARE aims to:

- Motivate IT administrators to reduce risk by comparing the scores of all endpoints in the responsibility of various administrators.
- Motivate management to support risk reduction by generally quantifying the amount of risk in one organization comparted to similar organizations.
- Measure improvement and/or performance by tracking risk, by organization, over time.

The CDM AWARE capability also allows security managers for participating agencies to compare their agency's risk score with average scores across the federal enterprise. In other words, an agency can see how its score compares to the average score across the Federal Government and how its score compares to the average score of equivalent agencies of similar size. Risk scores are calculated at the agency level and are then passed along to the CDM program, so no additional collection of agency data is required. The CDM AWARE capability does not introduce any additional privacy risks not already associated with the agency and federal CDM dashboards.

Privacy Impact Analysis

Authorities and Other Requirements

The operative authority for CDM is OMB Memorandum 19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements.*[7] The memorandum was released on October 25, 2018, and it noted that DHS will maintain a fully operational Federal Dashboard to provide situational awareness of the Federal Government's overall cybersecurity posture. Both CFO and non-CFO Act agencies are directed to establish the information exchange between their respective agency dashboards and the Federal Dashboard according to the timeline set forth by the CDM program.

[7] Office of Management and Budget Memorandum 19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, https://www.whitehouse.gov/wp-content/uploads/2018/10/M-19-02.pdf.

The current CDM Shared Service Platform received its authority to operate (ATO) on March 28, 2018. The CDM Shared Service Platform ATO remains active for three years, absent any significant system modifications, and is set to expire on March 28, 2021.

Characterization of the Information

There are no changes to the information collected by the CDM program. Some PII may be collected by departments and agencies that use CDM tools and services, however no PII is returned to CISA. Only high level summary data from each participating department and agency will be provided to the CDM federal dashboard managed by CISA. Each participating department and agency is responsible for its own systems and the protection of the information on those systems.

Uses of the Information

There are no changes to the uses of information as a result of the implementation of the CDM Shared Service Platform. CDM continues to be used to enhance the cybersecurity posture of federal networks and systems by employing continuous monitoring, diagnostics, and mitigation capabilities at federal departments and agencies. However, data collected by CDM tools and sensors within the shared service is provided to the respective department or agency through the integrator. This model is in contrast with the traditional deployment of CDM tools and sensors by federal departments and agencies on their own systems and networks where neither CISA nor any CISA funded parties (i.e., the integrator) have access to the department or agency's information other than the summary level information that is pushed to the federal dashboard.

The integrator does not provide any agency level dashboard information to CISA and works only to provide CDM shared services to participating departments and agencies.

Privacy Risk: There is a risk that PII inadvertently obtained by the integrator via the CDM Shared Service Platform will be used inappropriately.

Mitigation: The integrator is restricted from using information (including PII) not directly related to its deployment of the CDM Shared Service Platform for purposes beyond those specified by CISA in support of CDM. As a contractor to CISA, the integrator is required to conduct its activities in accordance with DHS requirements, including having all contract staff complete privacy training. Full disk encryption has been implemented across the entire shared service platform to meet applicable data-at-rest requirements. Additionally, all operational components of the shared service collect all logs at the operating system and application levels, including but not limited to, authentication, policy changes, permissions changes, and administrative changes. All users of the shared service (privileged and unprivileged) have been denied the ability to erase audit logs.

Notice

There is no change to notice practices as a result of the implementation of the CDM Shared Service Platform. Users of federal computer systems are provided with log-on banners and sign user agreements that specifically notify them of network monitoring for security purposes. This PIA also serves as a general notice to individuals that network traffic flowing to or from participating federal departments and agencies may be collected for security purposes.

Data Retention by the Project

There are no changes to the retention of CDM data as a result of the CDM Shared Service Platform. The CDM Federal Dashboard is hosted on CISA'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),[8] and August 6, 2015 (Records Schedule Number: DAA-0563-2015-0008).[9] Each participating agency is responsible for the management (to include retention) of its own network security information, including the information found on the Agency Dashboard.

Information Sharing

There are no changes to the information sharing practices as a result of the implementation of the CDM Shared Service Platform. CISA generates products on topics including general network security trends, specific incidents, and anomalous or suspicious activity observed on federal networks. However, specific individuals or entities are not identified in such products.

Redress

There are no changes to redress procedures as a result of the implementation of the CDM Shared Service Platform. There continue to be no procedures for individuals to correct information in the CDM Federal Dashboard because the CDM Federal Dashboard does not contain information on specific individuals.

[8] The NARA Record Schedule DAA-0563-2013-0008 is available at: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0008_sf115.pdf.
[9] The NARA Record Schedule DAA-0563-2015-0008 is available at: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2015-0008_sf115.pdf.

Auditing and Accountability

There are no changes to auditing and accountability capabilities as a result of the implementation of the CDM Shared Service Platform. The CDM Federal Dashboard does not collect PII and is the primary way in which CDM ensures information is being used in accordance with stated practices across federal departments and agencies.

Responsible Official

Jeanette Manfra
Assistant Director
Cybersecurity Division
Cybersecurity and Infrastructure Security Agency

Approval Signature

Original, signed copy on file with the DHS Privacy Office

_____

Jonathan R Cantor
Acting Chief Privacy Officer
Department of Homeland Security