United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Continuous Diagnostics and Mitigation (CDM)	
Preparer: David Stepp David Stepp (Federal OISP contact)	**Office:** EPA/OMS/OISP
Date: 5/14/2020	**Phone:** (202) 566-1611
Reason for Submittal: New PIA____ Revised PIA_X___ Annual Review__ __ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

The Office of Information Security and Privacy (OISP) manages a portfolio of applications, appliances, tools and sensors collectively referred to as the Continuous Monitoring (CM) System (Commonly referred to as CDM). Initial CM capabilities were introduced as part of the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program. The CDM program is being deployed to agency groups in a phased approach designed to defend Federal Government IT networks from cybersecurity threats and enhance risk-based decision making within agencies and across the Federal Government. This requirement, delineated in OMB Memo 14-03, requires Federal agencies to manage information security risks on a continuous basis, including a requirement to monitor the security controls in Federal information systems and the environments in which those systems operate.

The purpose of the CM system is to assist with defending the Agency IT network from cybersecurity threats and enhance risk-based decision-making. CDM utilizes tools and sensors to improve the Agency's abilities to analyze critical security-related information. CDM provides continuous monitoring networks for flaws and anomalies will alert network managers to attacks and exploitations, resulting in faster responses for problem mitigation.

Current capabilities deployed at EPA include credential management (CRED), configuration settings management (CSM), hardware asset management (HWAM), privileged access management (PRIV), software asset management (SWAM), and vulnerability management (VUL).

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

- OMB Directive 14-03 requires Federal agencies to manage information security risks on a continuous basis (every 72 hours), including a requirement to monitor the security controls in Federal Information systems and the environments in which those systems operate.
- 44 U.S.C. § 3506, which establishes federal agencies' responsibilities for managing information resources and 40 U.S.C. § 11315, which establishes the responsibilities of the agency's Chief Information Officer to manage agency information resources.
- Federal Information Security Modernization Act 2014 (FISMA) requirement for ongoing system security and is the means by which an organization shows due diligence in providing adequate security for its information and systems.
- The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, that establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes, a complete system security plan is maintained in EPA's governance risk and compliance tool (Xacta). The ATO expires on December 11, 2020.

1.3 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.

No ICR required. The provisions of the Paperwork Reduction Act are not applicable because information from members of the public is not collected.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

No

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 system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

The CRED and PRIV capabilities employ applications to utilize user data (from existing EPA defined authoritative sources), use (aggregate and normalize and then upload) disseminates (available for analysis on Agency CDM dashboard) and maintain (MUR data elements refresh rate is less than or equal to 72hrs). PRIV data elements are generated by the CyberArk application when a user is on-boarded. CyberArk serves as the authoritative sources for the data elements. Data elements develop a master user record (MUR) for everyone granted access to EPA facilities. A MUR is comprised of the data elements outlined in the table that follows

Table 1 MUR Data Elements

MUR Data Element	CDM Data Element	Key Identifier	Authoritative Source
IDENTITY			
Unique Identifier	Workforce ID	✓	eIDW
Full Name	None		eIDW
First Name	UserFirstName (optional)	✓	eIDW
Last Name	UserFamilyName (optional)	✓	eIDW
Middle Name	UserMiddleName (optional)	✓	eIDW
Generation Qualifier	None	✓	
Email	None	✓	eIDW
Job Title	UserJobTitle (optional)		eIDW
Department	OrganizationalUnitBoundaryID	✓	
Component	*OrganizationalUnitBoundaryID*	✓	eIDW
Location Attributes	None		eIDW
Manager	None	✓	eIDW
User Status	User Status	✓	eIDW
User Type	UserType	✓	eIDW
RMF Security Role	SecurityDutyID		eIDW
Date User Status Initiated	DateUserStatusInitiated		eIDW

MUR Data Element	CDM Data Element	Key Identifier	Authoritative Source
Date User Status Last Reviewed	UserReviewDate		eIDW
User Status Review Grace Period	UserReviewGracePeriod		eIDW
TRUST			
Trust Identifier	TRUSTID	✓	eIDW
Trust Status	TRUSTStatus	✓	eIDW
Name	None		eIDW
TRUST Description	TRUSTDescription		eIDW
TRUST Type	TRUSTType	✓	eIDW
Date TRUST Status Initiated	DateTRUSTStatusInitiated		eIDW
Date TRUST First Tracked	TRUSTCreationDate		eIDW
Date TRUST Expires	TRUSTExpirationDate		eIDW
TRUST Status Grace Period	TRUSTStatusGracePeriod		eIDW
Date TRUST Last Reviewed	TRUSTReviewDate		eIDW
TRUST Review Grace Period	TRUSTReviewGracePeriod		eIDW
BEHAVE			
Training Identifier	BEHAVEID	✓	Department of Interior (DOI) FedTalent LMS
Training Status	BEHAVEStatus	✓	DOI FedTalent LMS
Name	BEHAVE Element Name		DOI FedTalent LMS
Training Type	BEHAVEType	✓	DOI FedTalent LMS
Training Description	BEHAVEDescription		DOI FedTalent LMS
Date BEHAVE Created/Assigned	BEHAVECreationDate		DOI FedTalent LMS
Date Assigned BEHAVE expires	BEHAVEExpirationDate		DOI FedTalent LMS
Date BEHAVE Status Initiated/Changed	DateBEHAVEStatusInitiated		DOI FedTalent LMS
CRED			
CRED Identifier	CREDID	✓	eIDW
CRED Type	CREDType	✓	eIDW
CRED Status	CREDStatus	✓	eIDW
CRED Description	CREDDescription		eIDW
Date CRED Issued/Tracked	CREDCreationDate		eIDW
Date Issued CRED Expires	CREDExpirationDate		eIDW

MUR Data Element	CDM Data Element	Key Identifier	Authoritative Source
Date CRED Status Initiated	DateCREDStatusInitiated		eIDW
PRIV			
PRIV Identifier	PRIVID	✓	CyberArk
PRIV Type	PRIVType	✓	CyberArk
PRIV Status	PRIVStatus	✓	CyberArk
PRIV Description	PRIVDescription		CyberArk
Account Identifier	AccountID	✓	CyberArk
System Boundary Identifier	SystemBoundaryID	✓	CyberArk
Date PRIV Provisioned	PRIVCreationDate		CyberArk
Date Provisioned PRIV expires	PRIVExpirationDate		CyberArk
Date PRIV Status Initiated/Changed	DatePRIVStatusInitiated		CyberArk
PRIV Status Grace Period	PRIVStatusGracePeriod		CyberArk
PRIV Identifier	PRIVReviewDate	✓	CyberArk
PRIV Type	PRIVReviewGracePeriod	✓	CyberArk
ACCOUNT			
Account Identifier	AccountID	✓	eIDW
Account Type	AccountType	✓	eIDW
Account Status	AccountStatus		eIDW
Date Account Status Initiated	DateAccountStatusInitiated		eIDW
Account Status Grace Period	AccountStatusGracePeriod		eIDW
Account Creation Date	AccountCreationDate		eIDW
CRED Identifier	CREDID		eIDW

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

The CRED and PRIV capabilities receive data from EPA's Identity Data Warehouse (EIDW) and the Department of the Interior's (DOI) FedTalent Learning Management System. EIDW performs an automated data push to the CRED application, SailPoint. FedTalent data is collected from an EPA report and manually uploaded to SailPoint.

2.3 Does the system use information from commercial sources or publicly

available data? If so, explain why and how this information is used.

No

2.4 Discuss how accuracy of the data is ensured.

Data accuracy is the responsibility of and ensured by the authoritative data sources data owners. CDM assumes all data received authoritative and accurate. Detected data anomalies are reported to the respective data owner.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

There is risk that data may be accessed by unauthorized users or intentionally or un-intentionally exfiltrated.

Mitigation:

The system security plan outlines system level security controls in place to mitigate associated risks: Access Control (AC)-System access is limited to personnel with a need-to-know and Audit (AU)-system access is recorded and logged, administrative accounts are routinely reviewed and disabled if inactive. Enterprise/common controls are in place to monitor, detect and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Administrative access is granted only to qualified, trained individuals with a need-to-know. These users are granted elevated privileges and their accounts are regularly reviewed and audited. All administrative system actions are logged in accordance with audit security controls. Limited read-only user access is granted as well on need to know basis.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

EPA access control procedures outlined in CIO 2150-P-01.2 and are located here https://www.epa.gov/sites/production/files/2015-09/documents/cio-2150-p-01.2.pdf . System specific implementation of access controls are outlined in the system security plan.

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

Yes

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

A subset of EPA personnel, EPA contractors, DHS personnel and DHS contractors with a need to know may be granted read-only access to MUR data via the Agency CDM dashboard. Administrative access is limited to authorized EPA personnel and EPA contractors. External parties are not permitted administrative or elevated privileged access to MUR data.

EPA mandates the inclusion of FAR clauses in EPA service contracts.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

MUR data is refreshed at frequency less than or equal to 72hrs. Data may be retained as a result of system backups provided by the EPA hosting facility. System backups are retained for a period not to exceed 365-days. CDM system complies with EPA Records Schedule 0089.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

The longer records are retained the greater the likelihood data may be accessed by unauthorized users or data may be intentionally or un-intentionally exfiltrated.

Mitigation:

Data records are disposed of in accordance with EPA's record schedule 0089 retention requirements. The system security plan outlines additional system level security controls in place to further mitigate risk: Access Control (AC)-limits access to personnel with a need-to-know and Audit (AU)-system access recorded and logged, administrative accounts are routinely reviewed and disabled if inactive. Enterprise or common controls are in place to monitor and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

EPA shares the MUR data with the Department of Homeland Security (DHS) via the Agency and Federal CDM Dashboards. Data is used for compliance reporting, such as quarterly FISMA reporting. EPA entered into a Memorandum of agreement with DHS in 2014.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

The original purpose of the DHS CDM program is for Agencies to obtain and provide data to DHS. DHS utilizes the aggregation of the data to develop Agency and Federal Government risk profiles.

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

EPA's shares MUR data only with DHS and the arrangement is governed by the 2014 MOA. If any additional requests are made of the Agency, EPA will review and determine if appropriate revision to the MOA accordingly.

4.4 Does the agreement place limitations on re-dissemination?

Yes, data is not disseminated to entities other than DHS. Only aggregate data is provided via the Federal CDM dashboard. Under the CDM program EPA does not provide personally identifiable information to DHS.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

Expansive sharing of information increases the likelihood that data may be accessed by unauthorized users or data may be intentionally or un-intentionally exfiltrated. .

Mitigation:

Information sharing is limited to EPA and DHS, parties to the CDM Memorandum of

Agreement (MOA). The system security plan outlines additional system level security controls that are in place to enforce sharing limits: Access Control (AC)-limits access to personnel with a need-to-know and Audit (AU)-system access recorded and logged, administrative accounts are routinely reviewed and disabled if inactive. Enterprise or common controls are in place to monitor and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

Section 5.0 Auditing and Accountability

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

5.1 How does the system ensure that the information is used as stated in Section 6.1?

The system attempts to limit the misuse of information by first controlling access to the data. Access to data is limited to those with a demonstrated need to know and controlled by role assignment. The Agency has in place controls that limit the exfiltration of data further mitigating the likelihood of data misuse. System audit controls are also in place to record user actions relating to data use.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

All EPA Government Employees and contractors must complete EPA's Annual Information Security and Privacy Awareness Training. In addition, all users are required to read and sign the EPA Rules of Behavior that governs the appropriate use of information systems. Training is accessible via the Agency's FedTalent training web site.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Lack of or failure of auditing and accountability controls increases the likelihood that data may be accessed by unauthorized users or data may be intentionally or un-intentionally exfiltrated.

Mitigation:

The system security plan outlines system level security controls are in place: Access Control (AC)-limits access to personnel with a need-to-know and Audit (AU)-system access recorded and logged, administrative accounts are routinely reviewed and disabled if inactive. Enterprise or common controls are in place to monitor and respond to the exfiltration of user data: Incident Response (IR) and System and Information Integrity (SI).

Section 6.0 Uses of the Information

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

6.1 Describe how and why the system uses the information.

The Master User Records (MUR) contain records of users' statuses on the network and the associated implications for the security of systems within the agencies, which allows the Agency Dashboard to identify who is on an agency's network.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes ___ No _X_. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

The system purpose is not to perform retrieval based upon any personal identifier.

No, the system aggregates the raw data to develop a risk profile for who is on the network.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

Annually, system personnel: review the Privacy Impact Assessment, perform a risk assessment and undergo an independent security assessment that evaluates system security controls including privacy controls. The system only presents data that is already made available by the Agency. The data is used to develop a risk profile for the Agency based upon an aggregate of MUR data elements.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is risk associated with the use of information that the information may be accessed by unauthorized users or information may be intentionally or un-intentionally exfiltrated.

Mitigation:

An Annual security assessment is conducted to determine the efficacy of implemented security controls. Additionally, CDM regularly performs continuous monitoring activities to include configuration management settings audit and vulnerability scanning. A plan of actions and milestones (POA&Ms) is maintained to manage findings identified during these and other continuous monitoring activities.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

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

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

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 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.

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

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

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Mitigation: