Version Number: 01-2019

U.S. Department of Commerce
National Institute of Standards and Technology
(NIST)

Privacy Impact Assessment
for the
188-02 Enterprise Continuous Diagnostics and Mitigation (ECDM)

Reviewed by: Claire Barrett, Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 09/30/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
National Institute of Standards and Technology (NIST)

Unique Project Identifier: 188-02

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

a) Whether it is a general support system, major application, or other type of system
The Enterprise Cybersecurity Monitoring and Operations (ECMO) System (188-02) is an infrastructure system that provides enterprise-wide continuous monitoring capabilities across the Department of Commerce (DOC) and in support of the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program.

b) System location
The system is located at the NIST Gaithersburg, Maryland and Boulder, Colorado, facilities within the continental United States.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
The ECMO System obtains information (in flat files) from the following organizations:

- **Bureau of Economic Analysis (BEA)**
- **U.S. Census Bureau**
- **International Trade Administration (ITA)**
- **National Oceanic and Atmospheric Administration (NOAA)**
- **National Telecommunications and Information Administration (NTIA)**
- **NTIA FirstNet**

- **National Telecommunications and Information Administration (NTIS)**
- **Office of lnspector General (OIG)**
- **Office of the Secretary (OS)**
- **United States Patent and Trademark Office (USPTO)**

d) The way the system operates to achieve the purpose(s) identified in Section 4
The purposes of the ECMO components are to provide asset management, authenticated configuration, vulnerability, and patch scanning, as well as patch deployment, software deployment, and remote-control services, for DOC assets. Specific to privacy, the Continuous Diagnostics and Mitigation (CDM) functionality requires the management and control of four functions: account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE). In support of these functions, the ECMO creates and manages a Master User Record (MUR) for every person with access to participating DOC bureau networks. These functions are used to develop and maintain a Master User Record (MUR) for every person with access to participating agency networks. The MUR is built from identity data contained within various systems at participating agencies, includes data elements and attributes relevant to the functions, and centralizes pertinent information about a user and their relationship to applications and data. NIST has implemented the required components to accept data feeds from the participating DOC bureaus, as well as functionality to ingest, aggregate, and store those feeds for purposes of maintaining a MUR for those users using the existing NIST Shared Services Domain (SSDOC) infrastructure.

e) How information in the system is retrieved by the user
Information is retrieved by authorized users via a DHS commercial-off-the-shelf (COTS) identity management solution. The solution maps data elements to MUR required attributes and provides reporting capabilities for the information.

f) How information is transmitted to and from the system
Information is transmitted, in batch, to the system by participating DOC bureaus using protocols that provide encryption in transit, including Secure File Transfer Protocol (SFTP) and Transport Layer Security (TLS). Once received, the data is processed by matching a user's assigned DOC email address to update or create the record.

g) Any information sharing conducted by the system
The ECMO system does not share information.

h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
Federal Information Security Modernization Act of 2014 (44 U.S.C. 3551-3558) (FISMA)

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system is **High.**

Section 1: Status of the Information System

1.1 The status of this information system:

This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated.

Identifying Numbers (IN)
Employee ID*
Other identifying numbers:
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:
***Unique identifier attribute in the MUR, which is a government issued email address.**

General Personal Data (GPD)
Name
Other general personal data:

Work-Related Data (WRD)
Job Title **Work Address** **Work Telephone Number** **Work Email Address**
Other work-related data:

Distinguishing Features/Biometrics (DFB)
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
User ID **IP Address**
Other system administration/audit data:

Other Information

2.2 Indicate sources of the PII/BII in the system.

Directly from Individual about Whom the Information Pertains
Other:

Government Sources
Within the Bureau
Other DOC Bureaus
Other Federal Agencies
Other:

Non-government Sources
Other:

2.3 Describe how the accuracy of the information in the system is ensured.

The CDM performs validation checks prior to saving data submitted via the various interconnections to create a MUR for DOC users. Accuracy of the data submitted via interconnections is the responsibility of the participating DOC bureaus individually, as the bureaus run the source systems for that data.

2.4 Is the information covered by the Paperwork Reduction Act?

No, the information is not covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:

2.5 Is there any technology used that contain PII/BII in ways that have not been previously deployed?

No

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Other:

Section 3: System Supported Activities

3.1 Are there any IT system supported activities which raise privacy risks/concerns?

No

The IT system supported activities which raise privacy risks/concerns.

Activities

Other:

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.

Purpose
For administrative matters **Other**
Other:
To satisfy security requirements for the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program.

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The ECMO System provides enterprise-wide continuous monitoring capabilities across the Department of Commerce (DOC) and in support of the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program. All information collected is in reference to federal employee/contractors of DOC, including foreign nationals, who have access to a DOC system or network.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats include those between federal government organizations sharing data. Encrypted data controls at rest and in transit exist to mitigate this risk. **There is a risk that the collection of data from source agency systems may contain PII. This risk is mitigated by integrity checks by the source agencies.**

Section 6: Information Sharing and Access

6.1 Will the PII/BII in the system be shared?

No, the PII/BII in the system will not be shared

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Other:

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:

6.3 Identify the class of users who will have access to the IT system and the PII/BII.

Class of Users
Government Employees **Contractors**
Other:

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system.

No, notice is not provided.
The Privacy Act statement and/or privacy policy can be found at:
The reason why notice is/is not provided:
Notice is not provided as data is shared by the originating agency.

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

No, individuals do not have an opportunity to decline to provide PII/BII.
The reason why individuals can/cannot decline to provide PII/BII:
Individuals do not have an opportunity to decline to provide data as it is derived from the originating agency.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

No, individuals do not have an opportunity to consent to particular uses of their PII/BII.
The reason why individuals can/cannot consent to particular uses of their PII/BII:
Individuals do not have an opportunity to consent to particular uses of the data as it is derived from the originating agency.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

No, individuals do not have an opportunity to review/update PII/BII pertaining to them.
The reason why individuals can/cannot review/update PII/BII:
Individuals do not have an opportunity to review/update the data as it is derived from the originating agency.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system.

All users signed a confidentiality agreement or non-disclosure agreement. **All users are subject to a Code of Conduct that includes the requirement for confidentiality.** **Staff (employees and contractors) received training on privacy and confidentiality policies and practices.** **Access to the PII/BII is restricted to authorized personnel only.** **Access to the PII/BII is being monitored, tracked, or recorded.** **The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.** **The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.** **NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).** **A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.** **Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.**
Reason why access to the PII/BII is being monitored, tracked, or recorded:
Access logs are kept and reviewed for anomalies on an as needed basis.
The information is secured in accordance with FISMA requirements.
Is this a new system? No **Below is the date of the most recent Assessment and Authorization (A&A).** **10/04/2020**
Other administrative and technological controls for the system:

8.2 General description of the technologies used to protect PII/BII on the IT system. *(Includes data encryption in transit and/or at rest, if applicable).*

The components of the NIST-hosted CDM implementation reside within a restricted portion of the NIST network. Access to the network and CDM components is role-based and limited. Available settings within the CDM software components have been configured as restrictively as possible, only secure protocols are accepted, and only needed ports are open. Data is shared with CDM using a combination of SFTP, LDAPS, secure copy protocol (SCP), and TLS. Encryption at rest is implemented for the server that stores the source data feeds upon initial receipt, as well as for the supporting database where the data is ultimately stored. Audit logging functionality is fully enabled for all CDM components, functionality includes the generation of logs for security-related events, and alerts are generated for those events with significant security implications.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?
No, PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

No, this system is not a system of records and a SORN is not applicable.
SORN name, number, and link:
SORN submission date to the Department:

Section 10: Retention of Information

10.1 Are these records are covered by an approved records control schedule and monitored for compliance?

Yes, there is an approved record control schedule.
Name of the record control schedule:
GRS 3.2 Information System Security Records
The stage in which the project is in developing and submitting a records control schedule:
No, retention is not monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:
Data is referential.

10.2 Indicate the disposal method of the PII/BII.

Disposal
Deleting
Other disposal method of the PII/BII:

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

11.2 The factors that were used to determine the above PII confidentiality impact levels.

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Identifiability **Quantity of PII** **Context of Use**	**Identifiability-Information is non-sensitive.** **Quantity of PII-Masses of data from multiple bureaus are aggregated for trend analysis/reporting capabilities.** **Context of Use-This type of mass aggregation, "big data," could be sensitive if it were to fall into the wrong hands.**

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Unauthorized access to and/or disclosure of this data could have the following consequences: **• Grouping of aggregate data element patterns to aid in targeted attacks against DOC users and/or systems (e.g., attacks against users who rely on usemame/password authentication rather than PIV or attacks against users who have not completed cybersecurity training requirements).** **• Identification of privileged users (for DOC bureaus that provide such data). Targeted phishing attacks against those users could result in compromises and system failures of information services for those bureaus.** **These potential threats are mitigated with strong controls in place on the hosting servers and the controls protecting all of the components on the dedicated network that includes those servers. As no data elements on their own constitute sensitive PII, identity theft could not be performed in the event of unauthorized access to CDM data.**

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

No, the conduct of this PIA does not result in any required business process changes.
Explanation

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

No, the conduct of this PIA does not result in any required technology changes.
Explanation