

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



**Privacy Threshold Analysis  
for the  
188-02 Enterprise Continuous Diagnostics and Mitigation (ECDM)**

## U.S. Department of Commerce Privacy Threshold Analysis

### National Institute of Standards and Technology (NIST)

**Unique Project Identifier: 188-02**

**Introduction:** This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

**Description of the information system and its purpose:** *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines “information system” by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

- 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 purpose that the system is designed to serve*
- e) *The way the system operates to achieve the purpose*
- f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
- g) *Identify individuals who have access to information on the system*
- h) *How information in the system is retrieved by the user*
- i) *How information is transmitted to and from 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 Inspector General (OIG)
- Office of the Secretary (OS)
- United States Patent and Trademark Office (USPTO)

*d) The purpose that the system is designed to serve*

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).

*e) The way the system operates to achieve the purpose*

**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.**

*f) A general description of the type of information collected, maintained, use, or disseminated by the system*

Information contained within the attributes that comprise the MUR consists primarily of data found in the 'DOC Person Finder' (e.g., name, email address, phone number, and bureau), user metadata (e.g., status of training requirements and PIV status), and attributes identifying privileged users (for those DOC bureaus that provide that data). Unique identifiers are bureau-generated and are not derived from, nor consist of, personally identifiable information. There is no stand-alone sensitive Personally Identifiable Information (as an independent data element).

*g) Identify individuals who have access to information on the system*

**Information within ECMO is only accessible to authorized DOC users.**

*h) 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.**

*i) 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.**

**Questionnaire:**

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).**

*Skip questions and complete certification.*

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

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states “Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary.” Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

Activities
Other activities which may raise privacy concerns:

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: “For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as “trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential.” (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. “Commercial” is not confined to records that reveal basic commercial operations” but includes any records [or information] in which the submitter has a commercial interest” and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.).”

4. Personally Identifiable Information (PII)

- 4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 17-12: “The term PII refers to information that can be used to distinguish or trace an individual’s identity either alone or when combined with other information that is linked or linkable to a specific individual.”

The IT system collects, maintains, or disseminates PII about:

***If the answer is “yes” to question 4a, please respond to the following questions.***

- 4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

***If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.***

Is a PIA Required?	Yes
--------------------	-----

## CERTIFICATION

I certify the criteria implied by one or more of the questions above **apply** to the 188-02 Enterprise Continuous Diagnostics and Mitigation (ECDM) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

I certify the criteria implied by the questions above **do not apply** to the 188-02 Enterprise Continuous Diagnostics and Mitigation (ECDM) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):

Petrousky, Julia

Signature of SO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Co-Authorizing Official (Co-AO):

Signature of Co-AO: \_\_\_\_\_ N/A \_\_\_\_\_ Date: \_\_\_\_\_

Name of Chief Information Security Officer (CISO):

Heiserman, Blair

Signature of CISO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Authorizing Official (AO):

Sastry, Chandan

Signature of AO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Privacy Act Officer (PAO):

Fletcher, Catherine

Signature of PAO: \_\_\_\_\_ Date: \_\_\_\_\_

Name of Chief Privacy Officer (CPO):

Barrett, Claire

Signature of CPO: \_\_\_\_\_ Date: \_\_\_\_\_