Privacy Threshold Analysis
for the
Enterprise Cybersecurity Monitoring and Operations (ECMO)
System 188-02
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 of the information system in a way that a non-technical person can understand.

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

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), and
• 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. What is the status of this information system?

   ___ This is a new information system. *Continue to answer questions and complete certification.*

   **X** This is an existing information system with changes that create new privacy risks.
   *Complete chart below, continue to answer questions, and complete certification.*

<table>
<thead>
<tr>
<th>Changes That Create New Privacy Risks (CTCNPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Conversions</td>
</tr>
<tr>
<td>b. Anonymous to Non-Anonymous</td>
</tr>
<tr>
<td>c. Significant System Management Changes</td>
</tr>
<tr>
<td>d. Significant Merging</td>
</tr>
<tr>
<td>e. New Public Access</td>
</tr>
<tr>
<td>f. Commercial Sources</td>
</tr>
<tr>
<td>g. New Interagency Uses</td>
</tr>
<tr>
<td>h. Internal Flow or Collection</td>
</tr>
<tr>
<td>i. Alteration in Character of Data</td>
</tr>
</tbody>
</table>

   ___ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

   ___ 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 01-2015 or later). *Skip questions and complete certification.*

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.

   ___ Yes. *Please describe the activities which may raise privacy concerns.*

   **X** No

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.)."

____ Yes, the IT system collects, maintains, or disseminates BII about: (Check all that apply.)

____ Companies
____ Other business entities

X No, this IT system does not collect any BII.

4. Personally Identifiable Information
4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?
As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc."

X Yes, the IT system collects, maintains, or disseminates PII about: (Check all that apply.)

X DOC employees
X Contractors working on behalf of DOC
____ Members of the public

____ No, this IT system does not collect any PII.

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

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

X Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. 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.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.
No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c 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.
CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above apply to the Enterprise Cybersecurity Monitoring and Operations (ECMO) System (188-02), 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 Enterprise Cybersecurity Monitoring and Operations (ECMO) System (188-02), and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):
Matt Wilkinson
Signature of SO: ____________________________ Date: 9-21-2018

Name of Information Technology Security Officer (ITSO):
K. Robert Glenn
Signature of ITSO: ____________________________ Date: 9-20-18

Name of Co-Authorizing Official (AO):
Susannah Schiller, Acting
Signature of AO: ____________________________ Date: 9/20/18

Name of Co-Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO):
Susannah Schiller, Acting
Signature of AO/BCPO: ____________________________ Date: 9/20/18