Version Number: 01-2019

# U.S. Department of Commerce
# U.S. Patent and Trademark Office

## Privacy Threshold Analysis
## for the
## Enterprise Monitoring and Security Operations

# U.S. Department of Commerce Privacy Threshold Analysis

# USPTO Enterprise Monitoring and Security Operations

**Unique Project Identifier: PTOI-008-00**

**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:**

*a) Whether it is a general support system, major application, or other type of system*
Enterprise Monitoring and Security Operations (EMSO) is a General Support System.

*b) System location*
EMSO is located at 600 Dulany Street, Alexandria, VA 22314.

*c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
EMSO is a system that utilizes some of its subsystems to connect with all the USPTO systems. EMSO-SIEM and EMSO-PMT receives system and applications logs from all the USPTO systems.

*d) The purpose that the system is designed to serve*
EMSO is a product of many subsystems that have each functions, and they work together to provide an enterprise level monitoring system to the USPTO. Below is a description of each EMSO subsystem:

**Security Information and Event Management (SIEM)**

The SIEM provides a centralized command and control console with integrated enterprise log management, security information and event management, network behavior analysis, and reporting through the collection of events, network/application flow data, vulnerability data, and identity information. This solution consolidates events and data flows from a wide range of sources, and provides appropriate alerts on suspicious behavior to USPTO security, infrastructure, and operational personnel. The system does not actively collect PII, but it might incidentally store any potential PII if present within the collected logs. The system does not disseminate any collected potential PII data.

**Enterprise Forensic (EF)**

Enterprise Forensic is a network-enabled investigative infrastructure that enables Cybersecurity Investigators to conduct undetected/stealth PTO-wide in-house forensic computer investigations and hard drive (bit by bit) acquisitions over the network as well as Incident Response alerting capabilities. Enterprise Forensics provides immediate insight and awareness to threatened systems and information. EF performs state full inspection of incoming USPTO internet traffic to detect malicious software and cyber-attack signatures. The system does not actively collect PII, but it might incidentally copy any potential PII if present within the hard drive image being investigated. The system does not disseminate any collected data.

**Enterprise Management System (EMS)**

The Enterprise Management System (EMS) provides for automated, proactive system management and service-level management for application and database servers. The EMS AIS-supports high availability for all the USPTO servers and AIS software. This software provides EMS with the capabilities to perform automatic network device discovery, availability (up/down) monitoring, network mapping, data collections, reporting, and a centralized console to perform event correlation and alerting for all production USPTO network devices. The system does not collect, store or disseminate any PII data.

**Security and Defense (SD)**

Security and Defense provides connectivity for the USPTO network to reach applications, external devices, and networks which are not located on the Alexandria campus or not controlled by the USPTO. These include the Internet, Government sites, commercial sites, and contractor sites. Security and Defense also provides secure public and trusted users access to USPTO resources and applications.

The Security and Defense is responsible for maintaining the security and integrity of USPTO's internal (or private) network infrastructure while providing services for the public and partners of the USPTO, remote access for USPTO Staff, and connectivity to external systems and other Government agencies for USPTO staff. The system does not collect, store or disseminate any PII data.

**Enterprise Scanner (ES)**

Enterprise Scanner system provides agency-wide scanning capabilities such as vulnerability assessment, auditing compliance, configuration and patch management.

ES security scan tools are used to detect software vulnerabilities and ensure that information systems are compliant to USPTO baselines. Scans are performed on a quarterly basis for all information systems as part of continuous monitoring. The system does not collect, store or disseminate any PII data.

**Enterprise Cybersecurity Monitoring Operations (ECMO)**

OMB memoranda M-10-15 and M-10-19 require all Federal agencies to continuously monitor security-related information from across the enterprise and present this information to the various levels of agency-wide management to enable timely decision making. The Department of Commerce (DOC) - wide Enterprise Cybersecurity Monitoring and Operations (ECMO) initiative fulfills this requirement, providing near real-time security status, increasing visibility into system operations, and helping security personnel make risk-management decisions based on increased situational awareness. The DOC ECMO working group includes the United States Patent and Trademark Office (USPTO). The system does not collect, store or disseminate any PII data.

**Performance Monitoring Tools (PMT)**

Performance Monitoring Tools (PMT) utilizes a number of COTS products used by the Systems Performance Branch (SPB) to:

- Analyze USPTO-developed applications and PTONet Network performance to ensure performance objectives are being met.
- Establish and implement monitoring standards.
- Monitor existing capacity and project future capacity requirements.
- Formulate performance improvements and capacity changes.
- Recommend changes to systems, java virtual machines, databases, and PTONet to optimize application experience.
- Compile capacity and performance statistics for executive level reporting.

SPB is responsible for working with Systems Development Staff on architecting a standard performance monitoring and metric reporting system, as well as its upkeep and daily use within the CIO Command Center.

Additionally, PMT is used by SPB for conducting performance testing and analysis of applications prior to deployment, to devise methods to provide application availability metrics, and for alerting to the establishment and maintenance of the EMS. The system does not actively collect PII, but it might incidentally store any potential PII if present within the collected logs. The system does not disseminate any collected data.

**Dynamic Operational Support Plan (DOSP)**

The Dynamic Operational Support Plan (DOSP) is a centralized Operational Support Plan creation and display system. The DOSP has the capabilities of:

- Correlation, alignment, decomposition and pre-population of a product's system boundaries obtained from EMS network discovery and cybersecurity monitoring (CM) processes;
- Correlation and pre-population of a product's operational attributes based on manually entered values;
- Intake of configuration artifacts, formatted static text and images;
- Near real-time web publication and change tracking;
- Editing and viewing based on Role Based Access Controls (RBAC);
- Drafting and Approval functionality; and
- Archival ability.

The DOSP system uses web forms to intake product attributes provided by Technical Leads (TL) and various support groups. These values are stored in a centralized location within the EMS database. That data is then processed and aligned with already obtained network and CM data stored within the database and is used to publish a web accessible and RBAC controlled operational view of the product. The system does not collect, store or disseminate any PII data.

**Situational Awareness and Incident Response (SAIR)**

The Situational Awareness and Incident Response (SAIR) has implemented a technology platform to provide an Enterprise Common Operational Picture (ECOP) of the operational status of enterprise systems. ECOP provides enterprise situational awareness: the monitoring of the health and performance of devices and systems supporting PTOnet. The CIO Command Center (C3) provides the means from where the CIO, operational teams, Support Groups, and/or or designated CIO representative(s) can (either physically or virtually) view the ECOP, a near real time status of either internal and/or selected external events providing an enterprise-wide

Situational Awareness perspective from which to make decisions. This detailed enterprise-wide visibility is derived from the monitoring of IS's (information systems) in near real time. The system collects and stores SAIR personnel telephone numbers, but it does not disseminate any PII data.

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

Enterprise Monitoring and Security Operations (EMSO) utilizes its subsystems to perform its functions:

- **SIEM** consolidates events and data flows from a wide range of sources, and provides appropriate alerts on suspicious behavior to USPTO security, infrastructure, and operational personnel.
- **EF** provides immediate insight and awareness to threatened systems and information, revealing all data in RAM and on the hard disks regardless of efforts to hide or delete information.
- **EMS** performs automatic network device discovery, availability (up/down) monitoring, network mapping, data collections, reporting, and a centralized console to perform event correlation and alerting for all production USPTO network devices.
- **SD** maintains the security and integrity of USPTO's internal (or private) network infrastructure while providing services for the public and partners of the USPTO, remote access for USPTO Staff, and connectivity to external systems and other Government agencies for USPTO staff.
- **ES** provides agency-wide scanning capabilities such as vulnerability assessment, auditing compliance, configuration and patch management.
- **ECMO** provides near real-time security status, increasing visibility into system operations and helping security personnel make risk-management decisions based on increased situational awareness.
- **PMT** compiles capacity and performance data from the USPTO systems and applications, utilizes that data for monitoring network and application performance, and displays the overall health status.
- **DOSP** uses web forms to intake product attributes provided by TLs and various support groups. These values are stored in a centralized location within the EMS database. That data is then processed and aligned with already obtained network and CM data stored within the database and is used to publish a web accessible, and RBAC controlled, operational view of the product.
- **SAIR** provides an Enterprise Common Operational Picture (ECOP) of the operational status of enterprise systems. ECOP provides enterprise situational awareness and monitoring of the health and performance of devices and systems and/or supporting PTOnet.

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

EMSO, through its subsystems such as EMSO-SIEM and EMSO-PMT, receives and processes system and application logs from the all USPTO systems. Those logs are monitored for security related events and for the information system health status.

*g) Identify individuals who have access to information on the system*
Only a subset of authorized user such as the assigned system administrators have access to the subsystems with the potential PII data.

*h) How information in the system is retrieved by the user*
All users of EMSO are USPTO domain users. All EMSO users are separated into security groups having different levels of access based on their system role. All roles are defined and granted by the EMSO System Owner. Users with privileged accounts, or roles, with access to EMSO subsystems are managed, and only a subset of authorized users have access to the applications. EMSO users must logon to their workstations systems prior to authenticating to any of the EMSO system. Authorized privileged users access the applications for administrative functions only, and authorized non-privileged users access some applications as requirement for their roles within their group.

*i) How information is transmitted to and from the system*
Information is transmitted to and from EMSO via an internal USPTO network. EMSO system utilizes workstations, network devices, and servers to protect, monitor and scan the network, while providing an Enterprise Common Operational Picture to the C3 staff.

**Questionnaire:**

1. What is the status of this information system?

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

| **Changes That Create New Privacy Risks (CTCNPR)** | | | | | |
|---|---|---|---|---|---|
| a. Conversions | | d. Significant Merging | | g. New Interagency Uses | |
| b. Anonymous to Non-Anonymous | | e. New Public Access | | h. Internal Flow or Collection | |
| c. Significant System | | f. Commercial Sources | | i. Alteration in Character | |

| | | | | | |
|---|---|---|---|---|---|
| Management Changes | | | | of Data | |
| j. Other changes that create new privacy risks (specify): | | | | | |

_x__ 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). *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 01-2017 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. *(Check all that apply.)*

| **Activities** | | | |
|---|---|---|---|
| Audio recordings | | Building entry readers | |
| Video surveillance | | Electronic purchase transactions | |
| Other (specify): | | | |

__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.

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

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate 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."

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

- _x__ DOC employees
- ____ National Institute of Standards and Technology Associates
- _x__ Contractors working on behalf of DOC
- ____ Other Federal Government personnel
- ____ 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 Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates 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. |

_x__ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

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.

_x__ 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, 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.***

# CERTIFICATION

_x___ I certify the criteria implied by one or more of the questions above **apply** to the Enterprise Monitoring and Security Operations and as a consequence of this applicability, I will perform and document a PIA for this IT system.

Name of System Owner (SO): Michael Blevins

Signature of SO: Users, Blevins, Michael Digitally signed by Users, Blevins, Michael Date: 2020.03.20 10:09:52 -04'00' Date: _____

Name of Chief Information Security Officer (CISO): Don Watson

Signature of CISO: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2020.03.20 15:07:43 -04'00' Date: _____

Name of Privacy Act Officer (PAO): John Heaton

Signature of PAO: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2020.03.20 10:16:42 -04'00' Date: _____

Name of Authorizing Official (AO) & Chief Privacy Officer (BCPO): Henry J. Holcombe

Signature of AO & BCPO: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2020.03.20 17:45:25 -04'00' Date: _____