Version Number: 01-2017

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

Privacy Impact Assessment
for the
Enterprise Monitoring and Security Operations

Reviewed by: Henry J. Holcombe, Bureau 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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.10.15 14:48:42 -04'00' 03/18/2020

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Enterprise Monitoring and Security Operations

Unique Project Identifier: PTOI-008-00

Introduction: System Description

(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 its subsystems to connect with all the USPTO systems. Systems and applications logs are forwarded to SIEM and PMT.

(d) (d) The way the system operates to achieve the purpose(s)
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 subsystems:

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 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 including 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 projects future capacity requirements.
- Formulate performance improvements and capacity changes.
- Recommends 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, Performance Monitoring Tools are used by SPB for conducting performance testing and analysis of applications prior to deployment, devises methods to provide application availability metrics and 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 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
- 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 store SAIR personnel telephone numbers, but it does not disseminate any PII data.

(e) 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.

(f) 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.

(g) Any information sharing conducted by the system

EMSO subsystems do not share any information with any system. EMSO integrates with both the physical and logical access control systems to ensure the USPTO facilities and information systems are accessed by authorized personnel.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

Citation of the legal authority to collect PII and/or BII is 5 U.S.C. 301 and 35 U.S.C. 2

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

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

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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 Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

☒ 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.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	e. File/Case ID	☐	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☐
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☒	h. Alien Registration	☐	l. Vehicle Identifier	☐
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	☒	g. Date of Birth	☐	m. Religion	☐
b. Maiden Name	☐	h. Place of Birth	☐	n. Financial Information	☐
c. Alias	☒	i. Home Address	☐	o. Medical Information	☐
d. Gender	☐	j. Telephone Number	☒	p. Military Service	☐
e. Age	☐	k. Email Address	☒	q. Physical Characteristics	☐
f. Race/Ethnicity	☐	l. Education	☐	r. Mother's Maiden Name	☐
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	d. Telephone Number	☐	g. Salary	☐
b. Job Title	☒	e. Email Address	☒	h. Work History	☐
c. Work Address	☒	f. Business Associates	☐		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☒
b. IP Address	☒	d. Queries Run	☒	f. Contents of Files	☒
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	☐	Hard Copy: Mail/Fax	☐	Online	☐
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	Other Federal Agencies	☐
State, Local, Tribal	☐	Foreign	☐		
Other (specify):					

Non-government Sources					
Public Organizations	☐	Private Sector	☐	Commercial Data Brokers	☐
Third Party Website or Application			☐		
Other (specify):					

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

EMSO-SIEM and EMSO-PMT do not perform PII verification, if any is included within the logs data.
EMSO-EF captures hard drive image for investigation; however, the accuracy of any potential PII cannot be verified.
EMSO-SAIR might include a telephone numbers, which are entered and validated by users.

2.4 Is the information covered by the Paperwork Reduction Act?

☐	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
☒	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

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

Smart Cards	☐	Biometrics	☐
Caller-ID	☐	Personal Identity Verification (PIV) Cards	☐
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
To determine eligibility	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☐
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☐	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify):			

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).

EMSO-PMT receives application logs from applications running on servers within the USPTO. The data contained in the application logs ingested by PMT has three (3) major uses: to assist in evaluating and troubleshooting performance of a product; to help to identify and isolate transaction errors; and as a means to equate resource usage with business metrics. PMT retains the logs for at least 90 days before they are backed up by the USPTO backup system and maintained for 3 years. The incidental presence of any of the PII identified in section 2.1 could be from a federal employee/contractor.

EMSO-SIEM receives servers and applications logs within the USPTO. The logs contain system events and audit records. The logs are collected for security, events monitoring, and after-the-fact investigations. SIEM retains the logs for at least 90 days before they are backed up by the USPTO backup system and maintained for 3 years. The incidental presence of any of the PII identified in section 2.1 could be from a federal employee/contractor.

EMSO-EF collects hard drive image of a user's government issued laptop on ad hoc basis, whenever there is a Cyber and legal requirement. The hard disk image could possibly contain any of the items on 2.1 if a user has stored on the government issued laptop. The contents of a hard drive, while it is being extracted, stay within USPTO network boundary. The "image" is stored on servers which can only be accessed by a certain few individual within Cyber Security (6 total), they have their own firewall, and the physical server has its own server rack lock. The USPTO Cyber Security Investigations keeps possession of the "image" until that case closes. Once an investigation case has closed, then any potential PII data identified in section 2.1is destroyed. The incidental presence of any of the PII identified in section 2.1 could be from a federal employee/contractor.

EMSO-SAIR provide a template, for its personnel that are part of the USPTO incidence response team to provide their contact information (telephone number). The incidence response users have the opportunity to accept or decline to provide their personal telephone number. Only USPTO members of the incidence response team have access to any incidence response members' contact information. The telephone number could be from a federal employee/contractor.

5.2 Describe any potential threats to privacy 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.)

In the events of computer failure or an attack against the system, any potential personally identifiable information (PII) data from USPTO employees or contractors that are stored within the system could be exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network, and logical access is segregated with network firewall and switch through Access Control List that limits access to only a few approved and authorized accounts. The USPTO has SIEM systems that monitor in real-time all the activities and events within the servers storing the potential PII data, and a subset of USPTO C3 personnel review audit logs received on a regular basis and alert the ISSO and/or the appropriate personnel when inappropriate or unusual activity is identified.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☐	☐	☐
DOC bureaus	☐	☐	☐
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify):	☐	☐	☐

☒	The PII/BII in the system will not be shared.

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

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
☒	EMSO-SIEM and EMSO-PMT receives information (system and application logs) from the following other USPTO systems that have been authorized to process PII and/or BII: CAOS Corporate Administrative Office System (CAOS) Consolidated Financial System (CFS) Database Services (DBS)

	Enterprise Software Services (ESS) Fee Processing Next Generation (FPNG) IDP Information Delivery Product (IDP) Information Dissemination Support System (IDSS) Intellectual Property Leadership Management System (IPLMSS) Patent Capture and Application Processing System–Examination Support (PCAPS ES) Patent Capture and Application Processing System– Capture and Initial Processing (PCAPS IP) Patent End To End (PE2E) Patent Search System– Primary Search and Retrieval (PSS PS) Revenue Accounting and Management System (RAM) Trademark Next Generation (TMNG) The servers with the potential PII are located in a highly sensitive zone within the USPTO internal network, and logical access is segregated with network firewall and switch through Access Control List that limits access restricted to only a few approved and authorized accounts. The USPTO has applications and network appliances that monitor in real-time all the activities and events within the servers with the potential PII, and a subset of authorized USPTO C3 personnel review audit logs received on a regular basis and alert the ISSO and/or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis, utilization of Active Directory security groups to segregate users in accordance with their functions and the TACACS+ servers for authentication, authorization and accounting.
☒	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. EMSO-EF and EMSO-SAIR does not connect or receives any information from another USPTO systems.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	☐	Government Employees	☒
Contractors	☒		
Other (specify):			

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. *(Check all that apply.)*

☐	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☐	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____.	
☐	Yes, notice is provided by other means.	Specify how:
☒	No, notice is not provided.	Specify why not: EMSO-SIEM and EMSO-PMT collect systems and application logs, which contain system events and audit records for the management and monitoring of enterprise information systems. EMSO-EF is used for the acquisition of any hard drive (bit by bit) image for in-house forensic

		computer investigations. EMSO-SAIR is used for incidence response within the USPTO. No notice is provided because the systems have not been developed to collect PII data. It has the potential to store such PII data if they are included within the data being captured through the logs or image capture.

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

☒	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For EMSO-SAIR, users have the opportunity to accept or decline provide their PII information (telephone number). EMSO-EF users have the opportunity to accept or decline provide their PII information by not utilizing a USPTO laptop/desktop, used for the acquisition of any hard drive (bit by bit) image for in-house forensic computer investigations. It has the potential to store such PII data if they are included within the data being captured through the logs or image capture.
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: EMSO-SIEM and EMSO-PMT collect system and application logs, which contain system events and audit records for the management and monitoring of enterprise information systems.

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

☒	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: For EMSO-SAIR, users have the opportunity to consent that the information they provided could be used to contact them in an incidence response. EMSO-EF is used for the acquisition of any hard drive (bit by bit) image for in-house forensic computer investigations. It has the potential to store such PII data if they are included within the data being captured through the logs or image capture.
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: EMSO-SIEM and EMSO-PMT collect system and application logs, which contain system events and audit records for the management and monitoring of enterprise information systems.

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

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: EMSO-SAIR is used for incidence response within the USPTO, and the incidence response member can review and update their information (telephone number). EMSO-EF: Users can chose not to store any PII on their USPTO issued work laptop, and delete any content that they believe might contain PII, but if they chose to store PII data on the government issued equipment it belongs to USPTO until its destroyed. EMSO-EF is used for the acquisition of any hard drive (bit by bit) image for in-house forensic computer investigations. No notice is provided because the systems have not been developed to collect PII data. It has the potential to

		store such PII data if they are included within the data being captured through the logs or image capture.
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: EMSO-SIEM and EMSO-PMT collect systems and application logs, which contain system events and audit records for the management and monitoring of enterprise information systems.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☒	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. Explanation: Only authorized users have access to EMSO – SIEM, which collects the USPTO log files. Only authorized users have access to EMSO – EF, which collect forensics data on USPTO computers. Users access those applications using their USPTO domain credentials, and all the user's actions are recorded, tracked and monitored.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 3/29/19 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	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.
☐	Contracts with customers establish ownership rights over data including PII/BII.
☐	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

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

Information in EMSO is secured using appropriate administrative, physical, and technical safeguards in accordance with the applicable federal laws, Executive Orders, directives, policies, regulations, and standards. The servers with the potential PII are located in a highly sensitive zone within the USPTO internal network, and logical access is segregated with network firewall and switch through Access Control List that limits access restricted to only a few approved and authorized accounts. The USPTO has SIEM systems that monitor in real-time all the activities and events within the servers with the potential PII, and a subset of authorized USPTO C3 personnel review audit logs received on a regular basis and alert the ISSO and/or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis, utilization of Active Directory security groups to segregate users in accordance with their functions and the TACACS+ servers for authentication, authorization and accounting. All physical entrances to the datacenter are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pin code access screening. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. All users with access to the applications have been vetted and authorized by the System Owner, and the USPTO maintains an audit trail to identify authorized or unauthorized access. For EMSO – EF, individuals with the roles to capture image from hard drive for forensics investigation follow the chain of custody to ensure the potential PII data at rest is encrypted within the system, and that only authorized personnel have the authorization to access it. Personnel given roles in the SIEM system must be approved by the USPTO and complete training specific to their roles to ensure they are knowledgeable about how to protect potential personally identifiable information.

Section 9: Privacy Act

9.1 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."

☐	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*:
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☒	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: Non-recordkeeping copies of electronic records: GRS 5.1:020
☐	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
☐	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	☒	Overwriting	☒
Degaussing	☒	Deleting	☒
Other (specify):			

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

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 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.
☐	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☒	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: The information such as Name, address, phone number, email captured by the EMSO system could identify an individual.
☒	Quantity of PII	Provide explanation: Although EMSO systems were not developed to collect PII data, there is a potential for PII data to be included over time within the logs collected by the systems.
☒	Data Field Sensitivity	Provide explanation: Combination of name, address, phone number, email, and additional crash dump data may be more sensitive.

☒	Context of Use	Provide explanation: The SIEM and PMT subsystems collect applications logs, which contain system events and audit records. Data from the logs are the management and the monitoring of the information systems. The Enterprise Forensic (EF) application is used for the acquisition of any hard drive (bit by bit) image. Hard drive image are captured from hard drive images, when necessary, for PTO-wide in-house forensic computer investigations. The Situational Awareness and Incident Response (SAIR) is used for incidence response within the USPTO, and telephone number is use to contact personnel that are part of the USPTO incidence response team
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
☐	Access to and Location of PII	Provide explanation:
☐	Other:	Provide explanation:

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.)

In the events of computer failure or an attack against the system, any potential personally identifiable information (PII) data from USPTO employees or contractors that are stored within the system, could be exposed. Although EMSO systems have not been developed to collect PII data, there is a potential for PII data to be included within on the systems. USPTO personnel who are system users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers with the potential PII are located in a highly sensitive zone within the USPTO internal network, and logical access is segregated with network firewall and switch through Access Control List that limits access to only a few approved and authorized accounts. The USPTO has SIEM systems that monitors in real-time all the activities and events within the servers with the potential PII, and a subset of USPTO C3 personnel review audit logs received on a regular basis and alert the ISSO and/or the appropriate personnel when inappropriate or unusual activity is identified.

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

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

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

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.