Version Number: 01-2019

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

Privacy Threshold Analysis
for the
Storage Infrastructure Managed Services (SIMS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Storage Infrastructure Managed Services (SIMS)

Unique Project Identifier: [2941] PTOC-026-00

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: *Provide a general description system (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*
SIMS is a Major Application system.

b) *System location*
SIMS is located in Alexandria Virginia and Boyers Pennsylvania.

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
SIMS interconnects with the following USPTO systems: Network and Security Infrastructure (NSI), Enterprise Unix Services (EUS), Service Oriented Infrastructure (SOI), Agency Administrative Support System (AASS), Consolidated Financial System (CFS), Enterprise Desktop Platform (EDP), Information Delivery Product (IDP), Enterprise Records Management and Data Quality System (ERMDQS), Enterprise Windows Services (EWS), Information Dissemination Support System (IDSS), Intellectual Property Leadership Management Support System (IPLMSS), OCIO Program Support System (OCIO-PSS), Private Branch Exchange / Voice over Internet Protocol (PBX-VOIP), Patent Capture and Application Processing System - Initial Processing (PCAPS-IP), Patent Search System - Primary Search (PSS-PS), Enterprise Virtual Events Services (EVES), Enterprise Monitoring & Security Operations (EMSO), Trademark Processing System - External Systems (TPS-ES), Trademark Processing System - Internal Systems (TPS-IS), Contractor Access System (CAS), Enterprise Software Services (ESS), Personal Identity Verification Card Management System (PIVCMS), Patent Capture and Application Processing System – Examination Support (PCAPS-ES) and Patent Search System – Specialized Search and Retrieval (PSS-SS). SIMS has interconnection with the EMC Secure Remote Services (ESRS).

d) The purpose that the system is designed to serve
SIMS provides disk-based storage components, Storage Area Network (SAN), replication, and analysis capabilities.

e) The way the system operates to achieve the purpose
SIMS provides disk-based storage in two areas, block based storage and Network Attached Storage (NAS). Storage virtualization appliances support the mobility between data centers. Replication appliances copy data from the production site to the alternate processing site.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
Front end systems collect various data types which include identifying numbers, general personal data, work related data, distinguishing features/biometrics and system administration/audit data. The data is maintained in SIMS and supports dissemination.

g) Identify individuals who have access to information on the system
SIMS system administrators and USPTO government and contractor staff.

h) How information in the system is retrieved by the user
USPTO government and contractor users are granted access to repositories. Based on the access granted, users are able to read and/or write data.

i) How information is transmitted to and from the system
Authorized users access repositories to read, write or modify data based on permissions. The data from the repositories is replicated from the production site to the alternate processing site through dedicated replication appliances.

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 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. *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):			

☒ 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.)*

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

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."

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

- ☒ DOC employees
- ☐ National Institute of Standards and Technology Associates
- ☒ 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. The data stored in SIMS is based on the application/system ("front-end system") that uses SIMS for its storage requirements. For those systems that collect SSNs, their need for collection, maintenance, and dissemination is addressed by the front-end systems in their PIAs. SIMS does not directly collect SSN but it is a backend storage system that houses the information.
Provide the legal authority which permits the collection of SSNs, including truncated form. Executive Order 9397.

☐ No, the IT system does not collect, maintain, or disseminate SSNs, user ID is the only PII collected, maintained, or disseminated by the IT system.

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

☒ 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.

☐ 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

☒ I certify the criteria implied by one or more of the questions above **apply** to the Storage Infrastructure Managed Services 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 Storage Infrastructure Managed Services and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Ian Neil

Signature of SO: Users, Neil, Ian Digitally signed by Users, Neil, Ian Date: 2020.05.26 16:01:39 -04'00' Date: _____

Name of Privacy Act Officer (PAO): John (Ricou) Heaton

Signature of PAO: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2020.06.03 18:38:44 -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: 2020.06.08 18:23:42 -04'00' Date: _____

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

Signature of AO & BCPO: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2020.06.10 12:00:15 -04'00' Date: _____

Name of Authorizing Official (AO) or Designated Representative: N/A

Signature of AO: _____ Date: _____