Version Number: 01-2017

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

Privacy Impact Assessment
for the
Storage Infrastructure Managed Services (SIMS)

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

for Dr. Catrina D. Purvis LISA MARTIN Digitally signed by LISA MARTIN Date: 2019.08.30 17:20:42 -04'00' 07/06/2019

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Storage Infrastructure Managed Services (SIMS)

Unique Project Identifier: PTOI-027-00 (2941)

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

The SIMS storage infrastructure is spread across three (3) different data centers, each providing a specific role: the Alexandria Production Data Center (East), the Alexandria Test and Development Lab (West), and the Boyers (PA) Data Center. The SIMS architecture denotes the Boyers data center to be an alternate processing site, which is beyond its legacy storage component's current function as a data bunkering site. SIMS provides disk-based storage components, Storage Area Network (SAN), replication, and analysis capabilities. The disk-based storage components are separated into two main areas: 1) Block-based storage and 2) Network Attached Storage (NAS). The Block based storage is used to support the four Service Levels (Platinum, Gold, Silver, and Bronze). These service levels represent different levels of storage performance.

(a) a general description of the information in the system

Electronic data storage requires electrical power to store and retrieve that data. This electromagnetic data is stored in either an analog data or digital data format on a variety of media. This type of data is considered to be electronically encoded data, whether or not it is electronically stored in a semiconductor device, for it is certain that a semiconductor device was used to record it on its medium. Most electronically processed data storage media (including some forms of computer data storage) are considered permanent (non-volatile) storage, that is, the data will remain stored when power is removed from the device. For SIMS the stored data is based upon the application/system that possesses storage requirements. SIMS' systems stores data as files (predominantly) and support both Common Internet File System (CIFS) and Network File System (NFS) protocols. They can be accessed easily over the commonly used Transmission Control Protocol/Internet Protocol (TCP/IP) Ethernet based networks and support multiple users connecting to it simultaneously.

SIMS simply provides data storage for numerous USPTO information system-based applications and a list of those applications is located below in Section 6.2. These other systems use the data that is being stored in SIMS.

(b) a description of a typical transaction conducted on the system

A transaction usually means a sequence of information exchange and related work that is treated as a unit for the purposes of satisfying a request and for ensuring data integrity. For a transaction to be completed and data changes to be made permanent, a transaction has to be completed in its entirety. A typical transaction is an application request entered into a computer by an application

user. The request transaction involves checking a database, confirming that the data is available, placing the request, and confirming that the request has been placed and forwarded to the requestor.

If we view this as a single transaction, then all of the steps must be completed before the transaction is successful and the application database is actually changed to reflect the new order. If something happens before the transaction is successfully completed, any changes to the database must be kept track of so that they can be undone.

(c) any information sharing conducted by the system

When communities of interest share a physical SAN infrastructure, they can nevertheless keep their own traffic separate as it travels in and out of storage. Cisco director switches support multiple virtual SANs (VSANs) on the same physical SAN fabric. Each major application, for example, can have its own private VSAN, with its own encryption key, quality of service, security policies, and management functions. Employees can only connect to their own agency's VSAN, even though other agencies share the same physical SAN.

(d) a citation of the legal authority to collect PII and/or BII

5 U.S.C. 301, 35 U.S.C. 2, and 44 U.S.C. 3101.

(e) the Federal Information Processing Standard (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.)*
☒ This is an existing information system in which changes do not create new privacy risks. *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):					

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: The data stored in SIMS is based upon 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 those front-end systems in their PIAs. SIMS does not collect PIA but it is a backend storage system that houses the information.					
* If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished: Handling and usage of SSNs are addressed by the front-end systems. For those systems collecting SSNs, their approaches, where applicable, for avoiding collection, are identified within those systems' PIAs.					

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): SIMS is the enterprise-wide storage solution for USPTO * applications. If photographs are collected by a system, it is that application's responsibility to receive consent to collect and use.					

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 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).

SIMS stored data is based upon the application/system that is using SIMS for data storage. The information stored in SIMS is collected and utilized by USPTO application systems. SIMS does not collect PII but it is a back-end storage system that houses the information.

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: 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: • Corporate Administrative Office System (CAOS) • Consolidated Financial System (CFS) • Enterprise Software Services (ESS) • Personal Identity verification System Card Management System (HSPD-12/PIVS/CMS) • 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 Search System – Primary Search and Retrieval (PSS-PS) • Patent Search System – Specialized Search and Retrieval (PSS-SS) • Revenue Accounting and Management System (RAM) • Trademark Processing System – External System (TPS-ES) • Trademark Processing System – Internal System (TPS-IS) SIMS is on the USPTO network and adheres to the technical controls which are utilized by USPTO and outlined in the USPTO IT Security Handbook. SIMS is configured to protect data at rest (SC-28) through the separation of data streams across the arrays; thus, without knowledge of how the data has been sequenced, the information is unintelligible. Since data is located across multiple arrays, it lessens the risk of data loss.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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: SIMS houses the data that is stored via other application information systems within USPTO. These other systems provide this functionality for the data that is being stored. SIMS has no authorization to disseminate any type of information since that information is owned by the Application. Each of the systems housing information in SIMS provides individuals with notification on the front-end. SIMS is the enterprise-wide storage solution for USPTO applications. As a result if PII including photographs are collected by a system it is that application's responsibility to have the necessary privacy-related language including notice for giving consent to collect and use photographs.
☐	No, notice is not provided.	Specify why not:

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:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: SIMS houses the data that is stored via other application information systems within USPTO. These other systems provide this functionality for the data that is being stored. SIMS has no authorization to decline any type of information since that information is owned by the Application.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: SIMS houses the data that is stored via other application information systems within USPTO. These other systems provide this functionality for the data that is being stored. SIMS has no authorization to offer individuals the opportunity to consent to any type of information use since that information is owned by the Application.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: SIMS houses the data that is stored via other application information systems within USPTO. These other systems provide this functionality for the data that is being stored. SIMS has no authorization to review/update any type of information since that information is owned by the Application

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: Implementation of system auditing and monitoring functions is detailed in the SIMS SSP.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): June 8, 2018 ☐ 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 (POAM).
☒	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.

SIMS protects information and retains it within the system according to USPTO requirements and federal law. By default, data is written throughout the set of data drives within the storage array. Since data is located across multiple arrays, it lessens the risk of data loss. There is a different key for each drive in the storage array. The process occurs on the hardware, ensuring there is no possible way to reconstruct the specific data from a pattern of data scripting on multiple drives. Only administrators have access to the information, there are no user accounts on the system.

Restricting boundary traffic to SIMS infrastructure within managed interfaces and prohibiting external malicious traffic are the responsibility of the USPTO network infrastructure. They employ managed interfaces employing boundary protection devices including proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected sub-network referred to as a demilitarized zone or DMZ). This configuration protects the system from basic attacks like tear-drop, syn flood, smurf flood, ping flood and fraggle.

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, a SORN is not being created. SIMS simply stores data being used by other application information systems. Any record creation is the responsibility of the application information systems collecting and storing the information on SIMS.

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: The record control schedule is the responsibility of the application information system collecting the information. Refer to the application PIAs for more detail.
☐	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.

☐	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: Required credentials to identify the user when logging into storage.
☒	Quantity of PII	Provide explanation: PII that might be stored by the Application System. SIMS stores large quantities of data that may contain PII from across the USPTO network.
☒	Data Field Sensitivity	Provide explanation: PII or BII that might be stored by the Application System on the SIMS infrastructure.
☒	Context of Use	Provide explanation: PII or BII that might be stored by the Application System on the SIMS infrastructure.
☒	Obligation to Protect Confidentiality	Provide explanation: Sensitive data is located across different sections of the array and unintelligible without knowledge of all these locations. Since data is located across multiple arrays, it lessens the risk of data loss. As a repository for information from across the USPTO network, SIMS must ensure only authorized systems and individuals have access to their information.
☒	Access to and Location of PII	Provide explanation: Data that may be used, stored, and transmitted by the Application Systems is centrally stored by SIMS. SIMS must ensure that only authorized systems and individuals have access to their data from this central storage system.

☒	Other:	Provide explanation: System applications are responsible for determining the confidentiality impact levels collected, maintained, or disseminated by SIMS.

Section 12: Analysis

12.1 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.

12.2 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.