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

Jennifer Goode 02/25/2021

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: [2941] PTOC-026-00

<u>Introduction</u>: 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.

(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, Fee Processing Next Generation (FPNG) and Retrieval (PSS-SS). SIMS has interconnection with the EMC Secure Remote Services (ESRS).

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*
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.

(e) *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.

(f) *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.

(g) *Any information sharing conducted by the system*
SIMS provides disk-based storage for multiple USPTO information systems. Information is shared between the systems based on business needed. System heartbeats are shared with EMC ESRS for monitoring.

(h) *The specific programmatic authorities (statues or Executive Orders) for collecting, maintaining, using and disseminating the information*
5 U.S.C. 301, 35 U.S.C. 2, 44 U.S.C. 3101, Executive Order 9397.

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

☐ 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).

☐ 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).

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

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☒	o. Financial Information	☒
b. Maiden Name	☐	i. Place of Birth	☒	p. Medical Information	☐
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Physical Characteristics	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother’s Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	e. Work Email Address	☒	i. Business Associates	☒
b. Job Title	☒	f. Salary	☒	j. Proprietary or Business Information	☒
c. Work Address	☒	g. Work History	☒		
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
k. 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.

SIMS replicates the data from the production site to the alternate site. Weekly data backups are performed.

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. Application systems collect data covered by the Paperwork Reduction Act, SIMS supports the application by storing the data. SIMS depends on collecting systems to identify OMB control numbers on their PIAs.
☐	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			
For a Computer Matching Program	☐	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).

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 PII/BII, their need for collection, maintenance, and dissemination is addressed by the front-end systems in their PIAs.

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.)

Nation states and adversarial entities are the predominant threats to the information collected and its privacy. The system has implemented security controls following NIST guidance to deter and prevent threats to privacy. SIMS requires security awareness training, which covers appropriate handling of information and follows the USPTO media sanitization policy.

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: • Corporate Administrative Office System (CAOS) • Consolidated Financial System (CFS)

	- Enterprise Software Services (ESS) - Personal Identity Verification Card Management System (PIVCMS) - 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) - Fee Processing Next Generation (FPNG) - 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 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: https://www.uspto.gov/privacy-policy	
☒	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.
☐	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: Application systems collecting and SIMS storing PII/BII have a shared responsibility in monitoring, tracking and recoding access.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 12/6/2019 ☐ 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).*

SIMS protects information and retains it within the system according to USPTO requirements and federal law. By default, data is written throughout a 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. Data at rest encryption is available to applications/systems to that require it.

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. 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. *(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: PII that might be collected by the Application System and stored in SIMS can include SSN, First/Last Name, user ID, email, employee ID, financial account, file/case ID.
☒	Quantity of PII	Provide explanation: SIMS stores large quantities of data that may contain PII from across the USPTO network. Data is located across multiple arrays.
☒	Data Field Sensitivity	Provide explanation: PII that might be collected by the Application

		System and stored in SIMS can include SSN, First/Last Name, user ID, email, employee ID, financial account, file/case ID. Sensitive data is located across different sections of the array.
☒	Context of Use	Provide explanation: PII stored in SIMS supports multiple business unit applications. System applications are responsible for determining the confidentiality impact levels collected, maintained, or disseminated by SIMS.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data fields and in accordance with the Privacy Act of 1974, PII must be protected (SIMS is also contractually obligated to protect PII).
☒	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:

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.)

Nation states and adversarial entities are the predominant threats to the information collected and its privacy. Security controls following NIST guidance were implemented to deter and prevent threats to privacy. SIMS and system applications collecting the information have a shared responsibility in preventing and mitigating threats to privacy. SIMS is dependent on collecting systems to make decisions on data collection elements. Refer to the application PIAs for more detail.

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.