

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



**Privacy Impact Assessment  
For the  
Storage Infrastructure Managed Services (SIMS)**

Reviewed by: John B. Owens II, Senior Agency Official for Privacy

- Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
- Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

---

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-026-00 (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 component to be an alternate processing site, which is beyond its legacy storage'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 Block based storage and Network Attached Storage (NAS). The Block based storage is used to support the four Service Levels (Platinum, Gold, Silver, and Bronze). And their corresponding inputs and outputs (I/O) requirements and currently consists of an EMC VMAX 40K storage array. The NAS consists of an EMC Isilon system. The NAS component supports primarily the Silver Service Level. The SAN portion uses Cisco MDS and Nexus class hardware switches to provide connectivity between the storage components and the USPTO server environment. To support data mobility and replication between sites The SIMS relies on an EMC VPLEX storage virtualization appliance for data mobility within the Alexandria and Boyers data centers. Data replication between the Alexandria and Boyers sites is provided by EMC RecoverPoint appliances. The EMC RecoverPoint appliance allows for Continuous Remote Replication (CRR) as well as local and remote data protection, enabling reliable replication of data over any distance. The solution consists of enterprise class arrays with virtual storage technology that delivers data mobility and availability across the arrays for all of the defined storage classes at the Production, Boyers, and Lab environments.

*(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 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 CIFS and NFS protocols. They can be accessed easily over the

commonly used TCP/IP Ethernet based networks and support multiple users connecting to it simultaneously.

*(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 and entered into a computer by an application representative. 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 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.

SIMS' Storage Area Network (SAN) is a high-speed network of storage devices that connects those storage devices with USPTO servers. It provides block-level storage that can be accessed by the applications running on the networked servers. SIMS' SAN storage devices include arrays, tape libraries and disk-based devices, like RAID hardware. Block level access means, the server has the ability to create its own file system on SAN disk mapped to the server. SIMS employs transaction modeling, where each store has to be explicitly acknowledged from the remote node to be considered as successfully written. There may be lots of in-flight transactions. When remote host does not acknowledged the transaction it will be resent a predefined number of times with specified timeouts between them. These parameters are configurable. Transactions are marked as failed after all resends completed unsuccessfully, having long enough resend timeout and/or large number of resends allows not to return error to the higher (FS usually) layer in case of short network problems or remote node outages. In case of network RAID setup this means that storage will not degrade until transactions are marked as failed, and thus will not force checksum recalculation and data rebuild. In case of connection failure SIMS will try to reconnect to the remote node automatically.

*(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 agency or 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

For SIMS the stored data is based upon the application/system that possesses storage requirements.

(e) The Federal Information Processing Standard (FIPS) 199 security impact category for the system

<b>SIMS Security Categorization</b>	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.)

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
j. Other changes that create new privacy risks (specify): <b>No changes were made. This is a new template being used for the FY16 security authorization package.</b>					

**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.)

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

form: For SIMS the stored data is based upon the application/system that possesses storage requirements.

\*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:

**General Personal Data (GPD)**

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

**Work-Related Data (WRD)**

a. Occupation	<input type="checkbox"/>	d. Telephone Number	<input type="checkbox"/>	g. Salary	<input type="checkbox"/>
b. Job Title	<input type="checkbox"/>	e. Email Address	<input type="checkbox"/>	h. Work History	<input type="checkbox"/>
c. Work Address	<input type="checkbox"/>	f. Business Associates	<input type="checkbox"/>		
i. Other work-related data (specify):					

**Distinguishing Features/Biometrics (DFB)**

a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>	g. DNA Profiles	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>	h. Retina/Iris Scans	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>	i. Dental Profile	<input checked="" type="checkbox"/>
j. Other distinguishing features/biometrics (specify):					

**System Administration/Audit Data (SAAD)**

a. User ID	<input type="checkbox"/>	c. Date/Time of Access	<input type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input type="checkbox"/>	d. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
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	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
-----------	--------------------------	---------------------	--------------------------	--------	--------------------------

Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

<b>Government Sources</b>					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

<b>Non-government Sources</b>					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
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	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input type="checkbox"/>	To promote information sharing initiatives	<input checked="" type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input checked="" type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session )	<input type="checkbox"/>	For web measurement and customization technologies (multi-session )	<input type="checkbox"/>
Other (specify): For SIMS the stored data is based upon the application/system that possesses storage requirements.			

**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).

For SIMS the stored data is based upon the application/system that storage is provisioned. See the PIA for the USPTO information systems that utilize SIMS for storage. Relevant information regarding the PII/BII sent to SIMS is detailed in each of those documents. 5

**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	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.

<input checked="" type="checkbox"/>	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:
<input type="checkbox"/>	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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
Other (specify): For SIMS the stored data is based upon the application/system that possesses storage requirements.			

## **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.*)

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input type="checkbox"/>	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: _____.	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: System applications are responsible for notifying individuals if PII/BII is collected, maintained, or disseminated by SIMS.
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: System applications are responsible for providing individuals with an opportunity to decline, if PII/BII is collected, maintained, or disseminated by SIMS
<input type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: System applications are responsible for providing individuals with an opportunity to consent, if PII/BII is collected, maintained, or disseminated by SIMS
<input type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: System applications are responsible for providing individuals with an opportunity to review/update, if PII/BII is collected, maintained, or disseminated by SIMS
<input type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

**Section 8: Administrative and Technological Controls**

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

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>June 08, 2015</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	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).
<input type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	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, the VMAX Symmetrix writes data throughout the set of data drives within the storage array. There is a different key for each drive in the VMAX. The process occurs on the Disk adapter Serial Link 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."

<input type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> :
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input checked="" type="checkbox"/>	No, a SORN is not being created. System applications are responsible for creating a SORN on data levels collected, maintained, or disseminated by 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.)*

<input type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule:
<input checked="" type="checkbox"/>	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: Policy development. System applications are responsible for defining an approved records control schedule on data collected, maintained, or disseminated by SIMS
<input type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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.)*

<b>Disposal</b>			
Shredding	<input type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	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.)

<input type="checkbox"/>	Identifiability	Provide explanation:
<input type="checkbox"/>	Quantity of PII	Provide explanation:
<input type="checkbox"/>	Data Field Sensitivity	Provide explanation:
<input type="checkbox"/>	Context of Use	Provide explanation:
<input type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation:
<input type="checkbox"/>	Access to and Location of PII	Provide explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.