U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Storage Infrastructure Managed Services (SIMS)

DOC50PAPT0905000

05/29/2015

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

The Storage Infrastructure Managed Services (SIMS) is a detailed Storage Infrastructure which is designed for an extremely high level of availability, reliability, and resiliency, for blocks and file data types. The Storage Infrastructure is spread across three (3) different data centers, each providing a specific role; the Alexandria production data center, the Boyers data center, and the Test and Development Lab data center (Alexandria). The SIMS architecture denotes the Boyers component to be an alternate processing site, beyond the current function of a data bunkering site. The SIMS provides disk-based storage and consists of data center storage equipment that includes Storage Area Network (SAN) switches and storage devices consisting of Tier 1, Tier 2, and Network Attached Storage (NAS) devices. The Tier 1 SAN is used to support systems that require high-performance inputs and outputs (I/O) and currently consists of EMC a VMAX-40K storage array running higher performance drives.. The Tier 2 SAN supports systems that have less demanding I/O requirements, but is contained inside of the Tier 1 VMAX-40K storage array, comprised of lower performing disk drives. The NAS consists of EMC Isilon system. Other devices at the Alexandria location include EMC CLARiiON and Symmetrix storage arrays, and NetApp devices. There are currently four main types of devices at the Boyers site: EMC CLARiiON and Symmetrix storage arrays, and NetApp and EMC NAS devices. The SIMS relies on a data bunkering system (DBS) component for data replication between the Alexandria and Boyers sites. EMC RecoverPoint provides the 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.

QUESTIONNAIRE

1. What information is collected (e.g., nature and source)?

   Patent products include patent grants and patent application publications in image, text, text and image, and bibliographic forms; and additional information such as patent assignments, maintenance fee events, etc. Design Patents, Plant Patents, Reexamination Certificates (available only in Patent Grant Image files), Reissue Patents, Statutory Invention Registration (SIR) documents, Utility Patents. Trademark products include registration images, application text, assignment text, and Trademark Trial and Appeal Board (TTAB) text. Applicant names and addresses are collected as well.

2. Why is this information being collected (e.g., to determine eligibility)?

   The Patent organization examines patent applications to compare the scope of claimed subject matter to a large body of technological information to determine whether the claimed invention is new, useful, and non-obvious. Patent examiners also provide answers on applications appealed to the Board of Patent Appeals and Interferences (BPAI), prepare initial memoranda for interference proceedings to determine priority of invention, and prepare search reports and international preliminary examination reports for international applications filed under the *Patent Cooperation Treaty* (PCT).

   The Trademark organization registers marks (trademarks, service marks, certification marks, and collective membership marks) that meet the requirements of the Trademark Act of 1946, as amended, and provides notice to the public and businesses of the trademark rights claimed in the pending applications and existing registrations of others

3. What is the intended use of information (e.g., to verify existing data)?

   To determine whether the claimed invention is new, useful, and non-obvious and define trademarks, etc., to ensure infringements rights are protected.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

   USPTO provides notice to the public and businesses of the trademark rights claimed in the pending applications and existing registrations. Information may be shared with other NIST or Department of Commerce systems, in accordance with the Privacy Act.

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

   Users are notified of the USPTO privacy policy which states: we collect no personal information about you when you visit our website unless you choose to provide that information to us. Submitting personal information is voluntary. When you voluntarily submit information, it constitutes your consent to the use of the information for the purpose(s) stated at the time of collection. See the Privacy Act of 1974 (P.L. 93-579) for more information on your rights under the Privacy Act. Users who provide information to facilitate patent applications and trademarking are informed of the use of the information when it is requested and may decline to provide personal information. Businesses which contract with USPTO to perform patent applications and trademarking give their consent as part of the arrangements needed to complete these transactions.

6. How will the information be secured (e.g., administrative and technological controls)?
   As required by FIPS 199, the SIMS and its components were reviewed for the sensitivity of the information in them, and were determined to require protection appropriate for Moderate Impact systems. All relevant policies, procedures and guidelines, including NIST Special Publication 800-53, have been followed to ensure the security of the systems and the information in them. The System Security Plan on file with the SIMS Security Officer contains additional details. All users are authenticated via the domain and have password-sensitive screen savers enabled. All systems are running Antivirus software, desktop management software, and spy-ware elimination software. SIMS will also utilize PKI (Public Key Infrastructure) technologies and methods to secure information and transactions. Without proper identification (Customer Numbers and Digital Certificates) users are restricted to services such as pending application statuses or financial transactions. SIMS will also be accredited in accordance with Federal and Agency policies and guidelines.

7. How will the data extract log and verify requirement be met?
   Audit information for EMC storage systems is contained within the event log on each Storage Processor (SP). The log contains hardware and software debug information as well as audit information. It contains a time-stamped record for each event, and each record contains the following information:
   - ☐ Event code
   - ☐ Description of event
   - ☐ Name of the storage system
   - ☐ Name of the corresponding SP
   - ☐ Hostname associated with the SP

   The Storage Management Server adds audit records to the event log. An audit record is created each time a user logs in, enters a request through Unisphere, or executes a Secure CLI command. Each audit record is time-stamped, and identifies the following additional information for each request:
   - ☐ Requestor (Unisphere username)
   - ☐ Type of request
   - ☐ Target of request
   - ☐ Success or failure of request

   The Storage Management Server also restricts the ability to clear the audit log to administrators and security administrators only. Whenever the log is cleared by an authorized user, an event is logged to the beginning of the new log. This prevents users from removing evidence of their actions.

8. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?
   Yes, these records constitute a system of records within the meaning of the Privacy Act, and a system of records notice (SORN) is required

9. Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)?
   Records created by individual areas using SIMS are scheduled under National Archives and Records Administration (NARA) approved record retention schedules:

SIGNATORY AUTHORITY

Agreed: _____ 5/29/15

Ian Neil — Date

Information System Owner

Agreed: _____ 5/29/2015

John Pardun — Date

Senior Information Security Officer

Agreed: _____ 6/8/15

John B. Owens II — Date

Authorizing Official