

Department of State SharePoint Server PIA

1. Contact Information

A/GIS/IPS Director

Bureau of Administration

Global Information Services

Office of Information Programs and Services

2. System Information

- (a) Name of system: Department of State SharePoint Server
- (b) Bureau: IRM/OPS/SIO/CCS
- (c) System acronym: DoSSS-I & DoSSS-O
- (d) iMatrix Asset ID Number: 2741 & 2742
- (e) Reason for performing PIA:
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): System upgrade from Microsoft Office SharePoint Server 2007 (MOSS) to SharePoint 2010

3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
___ Yes ___X___ No
- (b) What is the security Assessment and Authorization (A&A) status of the system?
In progress. OpenNet ATO signed March 31, 2014; DMZ A&A documentation submission pending completion of the “pristine” DMZ environment
- (c) Describe the purpose of the system:

DoS SharePoint Services—(DoSSS-I and DoSSS-O) are the Department’s implementation of Microsoft SharePoint 2010. SharePoint is a multi-purpose online environment used for collaboration, content management, and web hosting. It is used both domestically and overseas by organizations throughout the Department. It features a suite of powerful collaboration, document management, database, and communication tools, as well as a high degree of integration with all Microsoft Office applications. In addition, SharePoint provides a secure, flexible platform on which to build custom web pages and applications. SharePoint functions primarily as a web

content management tool for displaying useful information to audiences within and outside of the State Department.

SharePoint is deployed in a central location from which users access content and applications through a web browser via the DMZ and OpenNet. The system's administrative functions and data are accessible only to authorized DoS personnel via either DMZ or OpenNet. Central administration and the hierarchical organization of SharePoint sites allow for the top-down application and enforcement of security restrictions. Role-based permissions are applied to all SharePoint entities—from the system as a whole down to individual files that are managed by local administrators known as Site Collection Administrators (SCAs).

This PIA will cover SharePoint sites that follow the guidance herein.

(d) Describe the PII that the system collects, uses, maintains, or disseminates:

SharePoint serves as a repository for collaborative information, which may include a variety of information from or about the public and Department workforce employees. The nature and sources of the information gathered depend upon the business needs of individual DoS organizations and initiatives as well as the laws and policies governing PII. The following information is an example of what may be collected by SharePoint sites:

- First Name
- Middle Name
- Last Name
- Maiden Name
- Email Addresses
- Title
- Phone Number
- Date of Birth/Place of Birth
- Gender (Male/Female)
- U.S. Citizen (Y/N)
- Social Security Number (U.S. citizens only)
- Passport Number
- Passport Issuing Country
- Photo
- Familial Contact Information
- Emergency Contact Information
- Biographic Information
- Mailing/Physical Addresses

Note: While IRM/OPS/SIO/CCS maintains the Department's SharePoint system, they do not own the data or processes stored within the system. Information contained in SharePoint is owned by the collecting office/bureau/post.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 22 U.S.C 2581 (General Authority of the Secretary of State).

Additional authorities governing the collection of PII by SharePoint sites or applications will be dependent on the functional authority of the office.¹

- (f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes X If yes, provide:

- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

No ___ If a SORN is not required, explain how the information is retrieved without a personal identifier.

Information included in the Privacy Act may be hosted on individual bureau site collections. Per the SharePoint Rules of Behavior any bureau retrieving records by a personal identifier is subject to provisions of the Privacy Act. The covering SORN for each SharePoint application varies by the mission of the office.¹

- (g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes ___ No X

If yes, please notify the Privacy Division at Privacy@state.gov.

- (h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? Yes X No ___

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)):
- Type of information retained in the system:
- Length of time the information is retained in the system:

Data collected and maintained by SharePoint serves different purposes for different business processes throughout the Department. Records retention and disposition vary by type of record collected. The record types will vary based on program needs. Information collected is maintained in accordance with data retention schedules appropriate to the specific activity and classification.¹

¹ Contact the Privacy Division for supplementary information about authorities, retention schedules and System of Records Notices (SORNs).

4. Characterization of the Information

- (a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other

- (b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

Yes No

- If yes, under what authorization?

Authorities governing the collection of SSNs by SharePoint sites or applications will be dependent on the functional authority of the office.²

- (c) How is the information collected?

Information would typically be collected on a voluntary basis via a web-based form or from a SharePoint list. Such forms could be as simple as the built-in SharePoint Survey feature or as sophisticated as a custom-programmed application front end. It is also possible that information could be entered by DoS administrative personnel reading from hardcopy forms. Another alternative would be to import the information from an electronic file such as an Excel spreadsheet, Word document or other document types that may be stored within a SharePoint repository.

- (d) What process is used to determine if the information is accurate?

Accuracy of the information is initially the responsibility of each bureau/office that collects and owns the information and subsequently enters it into SharePoint. In general, incoming information will be reviewed by Site Collection Administrators and any inconsistencies corrected by contacting the submitting individual submitting his or her information.

- (e) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Maintaining accurate information is the responsibility of each bureau or office using SharePoint.

- (f) Does the system use information from commercial sources? Is the information publicly available?
The uses of the information collected in SharePoint vary by the mission of the office.

- (g) Is notice provided to the individual prior to the collection of his or her information?
Notice is provided at the initial point of collection. Notice of the type of collection is also provided through the publication of the applicable SORN(s).

- (h) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? Yes No

- If yes, how do individuals grant consent?

² Contact the Privacy Division for supplementary information about authorities, retention schedules and System of Records Notices (SORNs).

The provision of information is strictly voluntary. However, if a user declines to submit the information, he/she may not be provided with the particular service he/she is requesting. SharePoint is typically used as a repository for information; therefore consent is given at the initial point of collection.

- If no, why are individuals not allowed to provide consent?

- (i) How did privacy concerns influence the determination of what information would be collected by the system?

To address privacy concerns in SharePoint, the Department published the SharePoint Rules of Behavior which require users to keep privacy in mind while using the application.

5. Use of information

- (a) The intended use(s) for the information is/are:

The collection and uses of the information are dependent upon the business needs of the bureau/office gathering the data. However, the following are examples of the purposes/uses for the information collected in SharePoint:

- Human Resource functions
- Resume/Biographic purposes
- Evaluations (on contractors)
- Family member data and onboarding procedures (at Post)
- Contests
- Event registration
- News feeds/letters/outreach
- Requests for information (external)
- Office collections of non-biographic personnel information
- Visitor information (to DoS facilities)
- Surveys
- Collaboration among Department offices
- Training purposes

- (b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

The purposes listed above are why SharePoint is used at the Department and what it was designed to handle.

- (c) Does the system analyze the information stored in it? Yes No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? Yes ___ No ___

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? Yes ___ No ___

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

SharePoint is a collaboration tool—it is designed to facilitate information sharing within the Department of State, so any office or bureau within the Department might collaborate with any other office or bureau as long as they have a need-to-know. PII will not be shared externally.

(b) What information will be shared?

Sharing of the information varies by the mission of the office within the scope of the Department's SharePoint regulations.

(c) The purpose for sharing the information is:

SharePoint is a collaboration tool—it is designed to facilitate information sharing within the Department of State.

(d) The information to be shared is transmitted or disclosed by what methods?

The information may be shared internally via the SharePoint application.

(e) What safeguards are in place for each internal or external sharing arrangement?

The safeguards for handling Sensitive But Unclassified (SBU) information, as listed in 12 FAM 544 will govern any internal sharing. PII will not be shared externally. Additionally, all information sharing is encapsulated within the SharePoint application, which has its own safeguards in place.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

The Fair Information Practice Principles (FIPPs), (minimization, notice, quality, access and redress, and protection) are considered when collecting, using and sharing the information. Additionally, the Department's SharePoint Rules of Behavior govern the application's uses. Sharing should only be done when there is a legitimate business need to do so.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals wishing to access and amend Privacy Act covered information collected by a SharePoint application follow the procedures defined in 22 CFR Subpart D 171 *Request to amend or correct records* at <http://2001-2009.state.gov/documents/organization/108115.pdf> or via the GPO at <http://www.gpo.gov/fdsys/pkg/CFR-2012-title22-vol1/xml/CFR-2012-title22-vol1-part171.xml>. In addition, full instructions for accessing and amending PII held by the Department

are available on the U.S. Department of State Freedom of Information Act (FOIA) website at <http://foia.state.gov/>. The site also provides complete information on FOIA, the Privacy Act, and related statutes and policies.

- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes No

If yes, explain the procedures.

Procedures vary by the mission of the office or bureau using SharePoint. Individuals should go back to the office or bureau responsible for the initial collection of their information for redress purposes.

If no, explain why not.

- (c) By what means are individuals notified of the procedures to correct their information?

Notification methods vary by the mission of the office or bureau using SharePoint. Individuals should go back to the office or bureau responsible for the initial collection of their information for redress purposes.

8. Security Controls

- (a) How is the information in the system secured?

The information collected is housed on secure servers.

- (b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

User roles are assigned by the bureau’s site administrator to limit access to only those who have an official need to know.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Audit logs are retained and must be reviewed by the bureau’s site administrator to prevent the misuse of the information.

- (d) Explain the privacy training provided to authorized users of the system.

All DoS employees, Federal and contractor, are required to complete annual cyber security training and certification in accordance with 5 FAM 1067.2 *Awareness, Training, Education and Professionalism (ATEP)*. SharePoint system administrators, site administrators, and application users are also required to read and sign the *Enterprise SharePoint 2010 Rules of Behavior* online form prior to accessing the environment.

- (e) Are any security controls such as encryption, strong authentication procedures, or other controls in place to make the information unusable to unauthorized users? Yes No

If yes, please explain.

- (f) How were the security measures above influenced by the type of information collected?
A minimal amount of information is collected to meet the mission of the each bureau.

9. Data Access

- (a) Who has access to data in the system?

- Internet use of SharePoint: General access control is provided by the DoS DMZ firewall. Users cannot access internal SharePoint administrative functions, application back ends, or databases from the Internet. Employee user access to specific SharePoint sites and SharePoint admin functions is controlled by role-based security permissions. SharePoint provides fine-grained security control down to the document level for individual users, user groups, and specific roles. Only users specifically provided with access to individual databases storing data collected via SharePoint (credentialing information, for example) will be able to view the data they contain. The existence of data and applications will be hidden from other SharePoint users not authorized to see them.
- Intranet use of SharePoint: General access control is provided by the DoS OpenNet firewall. Due to the single sign-on capability of OpenNet, users cannot access SharePoint administrative functions, application back ends, or databases from the Internet. Employee user access to specific SharePoint sites and SharePoint administrative functions is controlled by role-based security permissions. SharePoint provides fine-grained security control down to the document level for individual users, user groups, and specific roles. Only users specifically provided with access to individual databases storing data collected via SharePoint (credentialing information, for example) will be able to view the data they contain. The existence of data and applications will be hidden from other SharePoint users not authorized to see them.

- (b) How is access to data in the system is determined?

Access is determined by differing methods. External to the Department, users can not access collected data. Internally, access to collected data is role-based on a need-to-know basis.

- (c) Are procedures, controls or responsibilities regarding access to data in the system documented?

Yes X No

The Department published SharePoint Rules of Behavior to encapsulate these procedures, controls, and responsibilities.

- (d) Will all users have access to all data in the system or will user access be restricted? Please explain.

No. Users cannot access SharePoint administrative functions, application back ends, or databases from the Internet. Employee user access to specific SharePoint sites and SharePoint administrative functions is controlled by role-based security permissions. SharePoint provides fine-grained security control down to the document level for individual users, user groups, and specific roles. Only users specifically provided with access to individual databases storing data collected via SharePoint (credentialing information, for example) will be able to view the data

they contain.

- (e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Controls to prevent the misuse of data include the MOSS Rules of Behavior, mandatory cybersecurity training for all Department employees and contractors, privacy training, and the Department's Rules of Behavior for Protecting Personally Identifiable Information (PII).