1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: March 15, 2010

(b) Name of system: Department of State SharePoint Server - Internet

(c) System acronym: DOSSS-I

(d) IT Asset Baseline (ITAB number): 2741

(e) System description (Briefly describe scope, purpose, and major functions):

DoS SharePoint Services—Internet (DOSSS-I) is the Department's implementation of Microsoft SharePoint Server (MOSS) 2007 in the Internet DMZ. 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. As DOSSS-I, SharePoint functions primarily as a web content management tool for displaying useful information to audiences on the Internet. A secondary function is to enable secure data entry and data submission on the Internet.

DOSSS-I is deployed in a central location from which users access content and applications through a web browser. Although DOSSS-I websites and applications are Internet facing, the system's administrative functions and data are accessible only to authorized DoS personnel via OpenNet. Central administration and the hierarchical organization of DOSSS-I sites allow for the top-down application and enforcement of security restrictions. Role-based permissions can be applied to all DOSSS-I entities—from the system as a whole down to individual files.

(f) Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable): N/A, new system.

(h) Date of previous PIA (if applicable): N/A, new system.

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

Sharepoint serves as a repository for collaborative information, which may include a variety of information from or about the public. It is impossible to predict and enumerate the specific elements of PII that might be collected and processed by DOSSS-I applications. 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. Because the DOSSS-I Rules of Behavior forbid the handling of PII, websites or applications that do process PII are treated as exceptions on a case-by-case basis. The G-20 Summit press credentialing application is introduced here as an example of the kinds of data that can be collected and stored using SharePoint.

The G-20 website/application is currently inactive. It was commissioned by the White House and the Bureau of Public Affairs (PA) to gather information from members of the press wishing to attend the 2009 G-20 Summit in Pennsylvania. The information was used by the Secret Service[1] to conduct background checks of the applicants prior to issuing them photo ID badges for the event. This application may be reactivated for future G-20 summits or adapted for other events (e.g., the upcoming nuclear summit).

Utilizing the G-20 Summit web application, the following information may be collected by DOSSS-I:

- First Name
- Middle Name
- Last Name
- Email
- Media Title (Producer, Journalist, Photographer, Technician)
- Media Organization
- Organization Country
- Phone Number
- Date of Birth
- Gender (Male/Female)
- U.S. Citizen (Y/N)
- Social Security Number (U.S. citizens only)
- Passport Number (non-U.S. citizens only)
- Passport Issuing Country (non-U.S. citizens only)
- Photo

[1] For more information about the Secret Service's role in providing security for the G-20 summit, see http://www.secretservice.gov/press/GPA10-09_G20SecPlans.pdf.

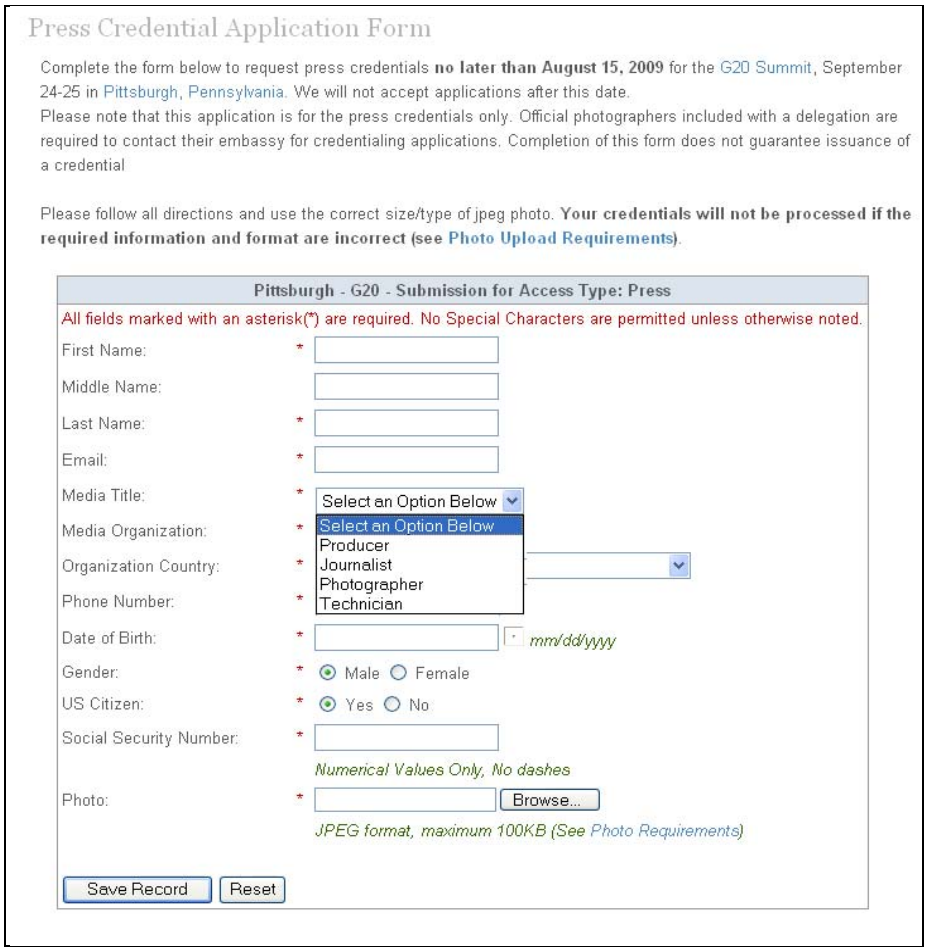
All form fields are required with the exception of Middle Name.

If the G-20 application is adapted for use in other contexts, the required fields may be different. Other DOSSS-I applications may handle additional data elements or fewer, but the information will typically be of the same general categories as those identified above. Addition of new data categories will require further analysis by the project team in cooperation with the Privacy Division (A/GIS/IPS/PRV).

b. How is the information collected?

Information from or about members of the public would typically be gathered via a web-based form. 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. At this time, the automated receipt of information from other computer systems via the Internet is neither anticipated nor authorized.

The G-20 example presented in (3a) makes use of a custom web form. The form itself is publicly accessible via the Internet. To provide his or her information, the prospective conference attendee accesses the form via the Internet, types the requested data into the form fields, and submits the form. Once the information is submitted, neither the person who filled out the form nor any other Internet user can access it again. The following screen shot illustrates the appearance of the G-20 web form for U.S. citizens:



Press Credential Application Form

Complete the form below to request press credentials **no later than August 15, 2009** for the G20 Summit, September 24-25 in Pittsburgh, Pennsylvania. We will not accept applications after this date.
Please note that this application is for the press credentials only. Official photographers included with a delegation are required to contact their embassy for credentialing applications. Completion of this form does not guarantee issuance of a credential

Please follow all directions and use the correct size/type of jpeg photo. **Your credentials will not be processed if the required information and format are incorrect (see Photo Upload Requirements).**

Pittsburgh - G20 - Submission for Access Type: Press

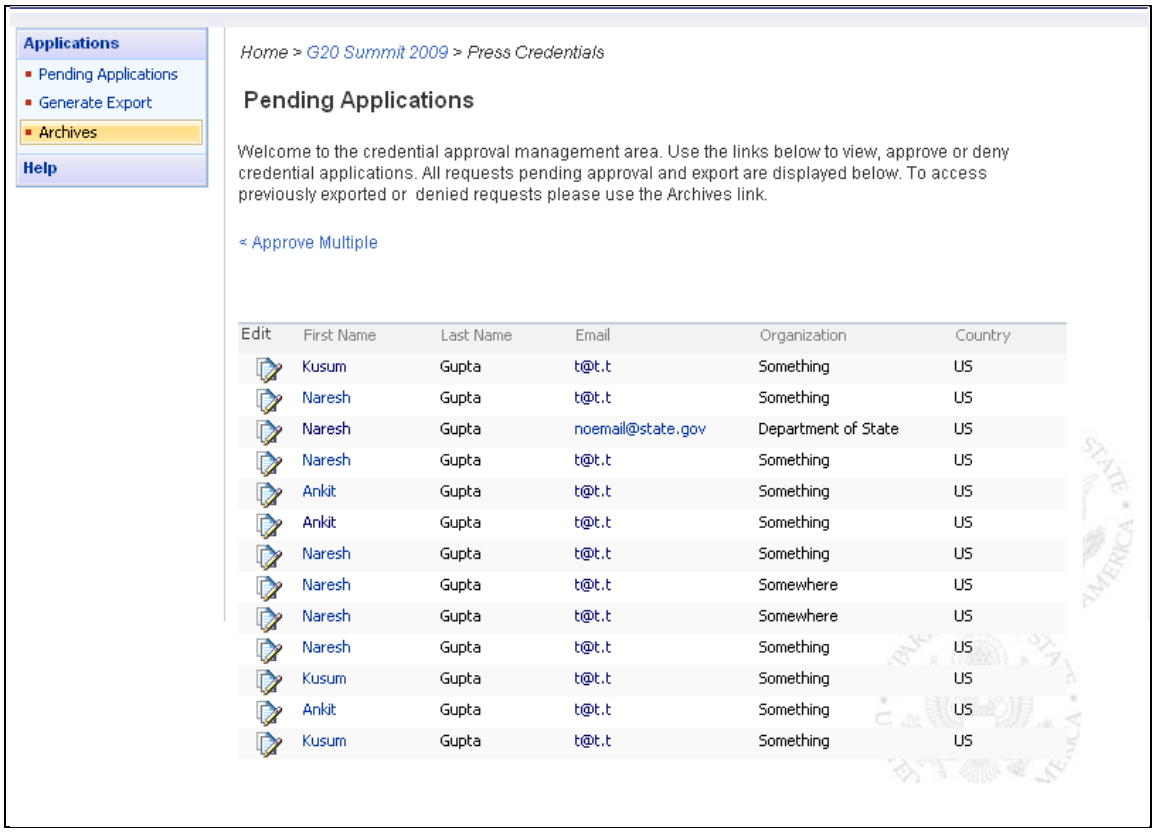
All fields marked with an asterisk(*) are required. No Special Characters are permitted unless otherwise noted.

First Name: *
Middle Name:
Last Name: *
Email: *
Media Title: * Select an Option Below
Media Organization: *
Organization Country: *
Phone Number: *
Date of Birth: * mm/dd/yyyy
Gender: * Male Female
US Citizen: * Yes No
Social Security Number: *
Numerical Values Only, No dashes
Photo: * Browse...
JPEG format, maximum 100KB (See Photo Requirements)

Select an Option Below
Producer
Journalist
Photographer
Technician

Save Record Reset

The information is then stored in a database on a secure server. Only SIO SharePoint system administrators (cleared American citizens with security awareness training and business need-to-know supporting the application) have direct access to the database. The organization/bureau collecting the data (in this case, Public Affairs) can review pending applications only through the application's administrative interface. Crucially, the administrative interface does **not** display any personally identifiable information. Public Affairs (PA) users only see the First Name, Middle Name, Last Name, Email, Organization and Country fields. Ultimately, only the U.S. Secret Service can actually see the PII contained in each credential request. The following screen shot illustrates the pending application list.



Edit	First Name	Last Name	Email	Organization	Country
	Kusum	Gupta	t@t.t	Something	US
	Naresh	Gupta	t@t.t	Something	US
	Naresh	Gupta	noemail@state.gov	Department of State	US
	Naresh	Gupta	t@t.t	Something	US
	Ankit	Gupta	t@t.t	Something	US
	Ankit	Gupta	t@t.t	Something	US
	Naresh	Gupta	t@t.t	Something	US
	Naresh	Gupta	t@t.t	Somewhere	US
	Naresh	Gupta	t@t.t	Somewhere	US
	Naresh	Gupta	t@t.t	Something	US
	Kusum	Gupta	t@t.t	Something	US
	Ankit	Gupta	t@t.t	Something	US
	Kusum	Gupta	t@t.t	Something	US

Thus, although PII is collected by the application, access to it is kept to an absolute minimum. It is expected that future applications will employ similar protections.

Alternatively, press organizations can submit information for multiple individuals by entering it into an Excel spreadsheet and emailing the spreadsheet to a secure DoS mailbox. The spreadsheet is uploaded to the application database, where the information it contains is handled the same way as information from the web form.

c. Why is the information collected and maintained?

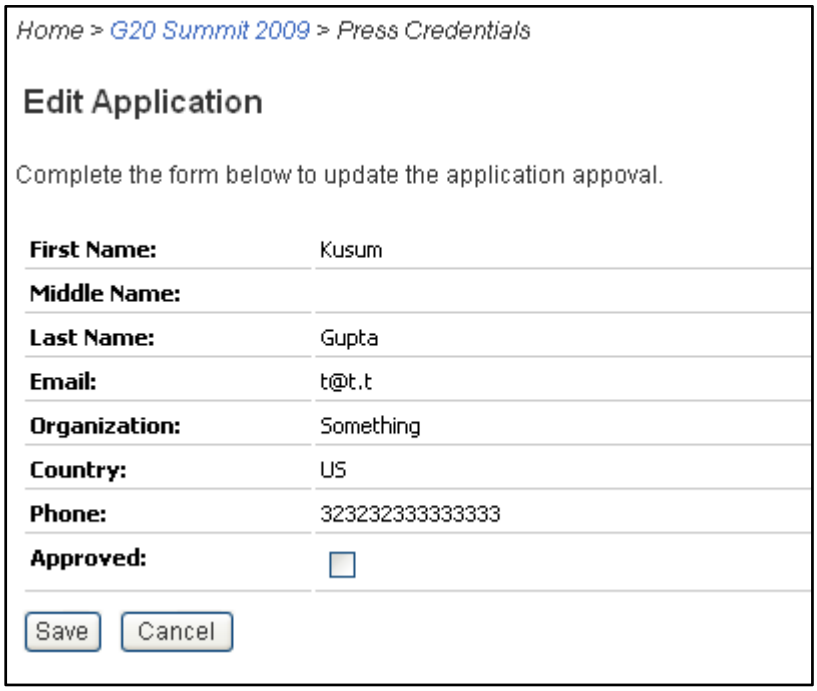
DOSSS-I is mainly used as a web content management tool for displaying information to audiences on the Internet. It can also be used to enable data entry and data submission on the Internet to support data analysis and data management by Department employees in support of credentialing and registration for international conferences and similar activities.

In the case of G-20 and similar applications, the information is collected for verification and validation in support of specific activities, and is maintained in accordance with data retention schedules appropriate to the specific activity (typically “Travel” and similar categories of data). The information is provided voluntarily by those individuals wishing to attend the event; the information is seen and used only by authorized personnel and only for the amount of time serving the occasion and retention regulations. At no point is information delivered to Internet viewers inside or outside the Department.

d. How will the information be checked for accuracy?

Accuracy of the information is initially the responsibility of the person entering the information. In general, incoming information will be reviewed by site or application administrative users and any inconsistencies corrected by contacting the submitting individual.

In the case of the G-20 application, the incoming information is checked by members of PA, with assistance from the White House Press Office if necessary. All validations are performed using the application's administrative interface on OpenNet. PA users have the ability to review and edit the **non-PII** portions of each request, correct any invalid information, and approve or deny the requests. The Edit screen is shown in the following screen shot:



e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 22 U.S.C. 2581 (General Authority of the Secretary of State).
- 1 FAM 275.5-3(C) Enterprise Collaboration Services (IRM/OPS/SIO/API/ECS)
- 5 FAM 777 Online Collaboration

Authorities governing the collection of PII by DOSSS-I sites or applications will be determined on a case-by-case basis. The following apply to the G-20 press credentialing application:

- 1 FAM 322.2-1 Office Of Press Relations (PA/PRS)
- 1 FAM 322.2-2 Foreign Press Centers (PA/FPC)

- Title 18, U.S.C. § 3056 (e)[1]

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

DOSSS-I serves various purposes and assists business processes throughout the Department of State. The most obvious risk is that PII could be displayed on the Internet—inadvertently or not. Numerous controls are in place to mitigate this risk. In common with other Department systems, DOSSS-I is protected by numerous management, operational, internal, and technical security controls implemented in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental security, encryption, role-based access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), annual training and audit reports.

In addition, the DOSSS-I Rules of Behavior (Sections 4.6, 4.7, and 4.8) explicitly prohibit the collection, storage, or transmission of PII within the system. Websites or applications that do process PII are treated as exceptions on a case-by-case basis. Organizations requesting such sites or applications must first demonstrate a valid business need for the PII, and are responsible for securing the necessary certifications and authorizations to operate. If necessary, a separate Privacy Impact Assessment will be completed for each individual application handling PII. Organizations are instructed to collect only the minimum amount of PII necessary to complete their statutorily mandated missions. Once the information is collected, access to it is restricted to a minimal number of authorized personnel on a need-to-know basis. Sites and applications collecting PII are typically deactivated when they are no longer needed. For example, the G-20 site is taken down once the deadline for submitting credential applications has passed.

4. Uses of the Information

a. Describe all uses of the information.

As with the types of information collected, it is also impossible to predict accurately the specific uses to which the information could be put. This depends mainly upon the business needs of the DoS organization gathering the data. However, PII is only used for the stated purpose for which it is collected. In the case of the G-20 conference application, PII voluntarily submitted by members of the press was forwarded to the Secret Service, which used it to conduct security background checks prior to issuing photo IDs for the conference. Based on the results of its investigations, however, the Secret Service may share the information with the Department of Justice and other law enforcement agencies.

---

[1] This title authorizes the Secret Service to participate in the planning, coordination, and implementation of security operations at special events of national significance, as determined by the President. The G-20 summit was such an event.

In accordance with the DOSSS-I Rules of Behavior, PII is never stored or displayed on the Internet. Users visiting DOSSS-I websites and applications from the Internet never have access to PII. When a specific application collects PII from Internet users, the data flow is strictly one way. That is, a user can enter PII, but once the information is submitted, may not view or edit it.

b. What types of methods are used to analyze the data? What new information may be produced?

The methods used to analyze the data depend upon the business needs of the organizations collecting the data. In the G-20 example, the Department and the White House validates the completeness and accuracy of the non-PII portions of the submitted data. If the information passes this basic validation, the application for press credentials is approved and sent on to the Secret Service. The Secret Service uses the information to conduct security background checks. No new information will be produced.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

DOSSS-I and the applications built on it currently do not use any of the types of information described.

d. Are contractors involved in the uses of the PII?

Yes. DOSSS-I is owned by DoS and its servers are maintained in a secure federal facility. Contractors are involved in the design, implementation, operation, use, and maintenance of DOSSS-I websites and applications. All contractors possess at minimum a Secret security clearance; they have also passed a National Agency Check and Diplomatic Security Processing. All contractors have an approved Privacy Act clause in their contracts and must pass annual security/privacy training.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Physical control is provided by DoS network security protocols already in place and by applicable DoS and security and privacy regulations (i.e., 5 FAM 400 and 5 FAH 4). All DoS SharePoint users receive the Department's mandatory IT security and privacy training as a condition of their access to OpenNet. Owners and administrators of all SharePoint websites and web applications are also subject to the DOSSS-I Rules of Behavior (see Attachment 1), which specifically address privacy and appropriate use.

All authorized users must pass annual computer security and privacy training. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Furthermore, system audit trails are automatically generated and regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of the particular functions a particular user performed--or attempted to perform.)

In addition to the common protections described above, applications operating in the DOSSS-I environment are governed by their own programmatic controls and rules of behavior. For example, the G-20 application's administrative interface does not allow users to view or alter PII submitted by requesters. In addition, users are restricted from viewing the Excel file that is sent to the Secret Service. Ultimately, only the Secret Service is able to view PII from the G-20.

5. Retention

a. How long is information retained?

Data collected and maintained by DOSSS-I 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 is maintained until it becomes inactive or is no longer needed for the purpose for which it was collected. (In the G-20 example, as soon as the conference registration deadline has passed.) At that point, records containing the information are destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). The current Records Disposition Schedule is available at http://infoaccess.state.gov/recordsmgt/recdispsched.asp.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Any risks associated with data retention are adequately addressed by document publishing and aging controls provided by MOSS as well as the document control and retention procedures specified in 5 FAM 400 and 5 FAH 4, and the Department's NARA-approved records disposition schedules.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

DOSSS-I is a collaboration tool—it is designed to facilitate information sharing within the Department of State. Potentially, any DoS bureau or post using DOSSS-I can share information with any other. Currently, no uses of DOSSS-I involve sharing PII among DoS organizations. Specific data-sharing arrangements are handled on a case-by-case basis. In the case of G-20, the information is limited to use by authorized personnel of the Bureau of Public Affairs.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Currently, no uses of DOSSS-I involve sharing PII among DoS organizations. Should the need for such sharing arise, the process will be conducted via secure network connections on OpenNet, SIPRNet, or ClassNet.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

One of the primary purposes for the implementation of DOSSS-I is to increase collaboration across all bureaus within the Department. The handling of PII in such a collaborative environment—especially one connected to the Internet—obviously brings with it the risk of unauthorized access to or exposure of private information. To mitigate this risk, the DOSSS-I Rules of Behavior (See Attachment 1) explicitly forbid the posting or storage of PII anywhere on the system. In cases where organizations need to collect PII from members of the public (e.g., the G-20 application), the information is stored and processed on servers in the OpenNet or other secure environment, not in the Internet DMZ. Access to such information is limited to authorized DoS personnel on a need-to-know basis. Any information sharing arrangements between DoS organizations are made on a case-by-case basis with due regard for privacy risks.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Data stored in DOSSS-I will not be directly accessible to users or computer systems external to the Department. DoS organizations can use SharePoint websites and applications to display non-PII information to audiences on the Internet.

Currently, only the G-20 press credentialing application collects PII to be shared with outside organizations—in this case the Secret Service. The information is used to conduct background security checks in compliance with the Secret Service's statutorily mandated mission. Only the Secret Service has access to the PII portions of each credential request via an Excel spreadsheet file. The G-20 application hides PII from all other users.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

The G-20 application has the ability to export press credential data to a Microsoft Excel spreadsheet. The spreadsheet is then made available to the Secret Service on a secure server behind the OpenNet firewall.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

It is anticipated that any future information sharing between DOSSS-I and outside organizations will occur via secure servers and secure network connections on OpenNet, ClassNet, or SIPRNet.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

A Statement of Record Notification (SORN) is being developed. When complete, it will be submitted to Privacy Division along with an updated, signed copy of this PIA.

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Yes. In accordance with SIO SharePoint web design standards, each application displays a statement providing the user with full information about the private nature and intended use of the information being requested. (See Attachment 2, Privacy Act Statement.) In addition, contact information is provided in case the user has questions regarding the intended use of the data.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes. The provision of information is strictly voluntary. However, if a user declines to submit the information, they may not be provided with the service they are requesting—e.g., the issuance of press credentials.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. Individuals may either submit or decline to submit the requested information. In general, DOSSS-I applications are intended to collect information for specific and clearly defined purposes—e.g., the issuance of press credentials.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

SIO SharePoint web application design standards greatly reduce the risk that a user would be unaware that PII is being collected. Each application displays full information

about the purpose of collecting the PII and its intended uses. (See Attachment 2, Privacy Act Statement, for an example.) In order to provide the information, the user must intentionally navigate to the application, type the information into the form fields, and press a "submit" button. In addition, the G-20 application specifically informs the user that once they submit their information it will no longer be accessible to them for correction or withdrawal.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals wishing to access or amend privacy act information collected by a DOSSS-I application follow the procedures defined in 9 FAM 40.4 N4 *FOIA and Privacy Act Requests*. 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://www.state.gov/m/a/ips/. The site also provides complete information on FOIA, the Privacy Act, and related statutes and policies.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

General access control is provided by the DoS Internet firewall. Users cannot access DOSSS-I administrative functions, application back ends, or databases from the Internet. Employee user access to specific DOSSS-I sites and DOSSS-I admin functions is controlled by MOSS role-based security permissions. MOSS 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 DOSSS-I (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. What privacy orientation or training for the system is provided authorized users?

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)*. DoSSS-I system administrators, site

administrators, and application users are also required to read and sign the *DOSSS-I Rules of Behavior* (ROB) online form prior to accessing the environment. A copy of the ROB text is provided as Attachment 1.

In addition, all Department personnel are given a brief security quiz each time they log onto OpenNet. Content is randomly generated, and covers physical security, info security, classified handling, etc. The quiz includes questions very specific to the protection of personally identifiable information and Privacy Act data.

For members of the public, if requested to input information into the system, detailed instructions are available on the website. The application also provides public users with instructions for contacting application owners for further information. In the case of applications collecting PII, a privacy statement displayed before the user enters any information. (See Attachment 2, Privacy Act Statement.)

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Unauthorized access by users from the Internet is minimal. However, due to the availability of information on DOSSS-I to almost all authorized DoS OpenNet users, there is a significant risk of unauthorized access from within DoS. This risk is minimized through the use of internal network, SharePoint, and application security controls, rules of behavior, and proper IT security training of all OpenNet users.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

DOSSS-I is a secure environment hosted on the OpenNet network. It does not employ any new technology and relies on existing OpenNet and SharePoint security controls.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

DOSSS-I relies on existing networking technology and does not employ any hardware or software that increases privacy risk.

12. Security

What is the security certification and accreditation (C&A) status of the system?

DOSSS-I is currently undergoing C&A. Anticipated completion: March 2010.

Attachment 1

DOSSS-I Rules of Behavior

1. Introduction

The Office of Management and Budget (OMB) Circular A-130, Appendix III Security of Federal Automated Information Resources requires that 'Rules of Behavior' be established for each general support information technology system and major application processing government information. The Rules of Behavior delineated below pertain to all persons who utilize the DoS SharePoint Services (DOSSS) web portal, which is an IT resource for the Department of State (DoS). The following Rules of Behavior and acceptable use policy apply to all administrators and contributors of the DOSSS environment whether they are DoS employees, contractors or members of external agencies.

The Rules of Behavior provide general instructions on the appropriate use of the DOSSS and specifically apply to the following SharePoint sites and their respective sub-sites:

SharePoint Bureau and Post Sites (http://collaborate.state.gov)

These sites may be on any of the following networks:

SharePoint OpenNet

SharePoint OpenNet Demilitarized Zone (DMZ)

SharePoint ClassNet

SharePoint ClassNet Demilitarized Zone/SIPRNet (DMZ)

Groove OpenNet

Groove ClassNet

2. Other Policies and Procedures

The Rules of Behavior are not to be used in place of existing policy or guidelines. Rather, they are intended to supplement the DoS Information Security Program Policy and the DoS Information Security Program Handbook. Because written guidance cannot cover every contingency, Department staff is asked to augment these rules and use their best judgment and highest ethical standards to guide their actions.

As with any intranet website ,users must adhere to the following DoS website guidelines: 5FAH-8 H-100 , 5FAH-8 H-200 , 5FAH-8 H-400 , 5FAH-8 H-430 , 5FAH-8 H450, 5FAM 770

Additionally for internet-hosted sites users must adhere to the following Guidelines for Public Information Dissemination on the Internet: http://iip.r.state.sbu/ISC/default.aspx

3. SharePoint Overview

SharePoint allows you to:

Store your organization's documents and information securely

Collaborate on documents and reports

Manage content and streamline processes

Build collaboration and published website for information sharing and or marketing purposes

Search for documents, sites, and SMART Archival Messages

Share information and collaborate internally (within DoS on ClassNet and OpenNet) and externally (with external agencies on SIPRNet and NIPRNet) across network boundaries

4. SharePoint Rules of Behavior

4.1. Administrators must be assigned by Bureau or office advocates.

4.2. Contributors and users must be assigned by the site administrator.

4.3. Administrators can give contributors access to those individuals that have agreed to the Rules of Behavior and require the use of SharePoint to solve a business need.

4.4. Users must follow a configuration management process for storing information and data on the SharePoint sites.

4.5. .Administrators are responsible for the management of site content at the top-level site and at the sub-site levels. Administrators may re-assign the responsibility of Content Manager to those individuals who manage particular sub-sites.

4.6. Users cannot post combinations of key privacy information or combinations of Personally Identifiable Information (PII) on the OpenNet Demilitarized Zone (DMZ). If PII needs to be posted on OpenNet, ClassNet, or SIPRNet, that information needs to be restricted to users on a "need-to-know" basis.

4.6.1. These combinations could include full name, birth date, social security number, or address.

4.7. Users should not post items that will affect the National Security of the Department of State or any collaborating agencies.

4.7.1.1. Examples of non-acceptable information include: Social Security Number + Last Name (or any combination of SSN with other PII, i.e. date of birth, phone number, and first name)
4.7.1.2. Communications, contracts, or negotiations regarding external affairs
4.7.1.3. Architectural drawings or floor plans related to DoS facility (embassies, consulates, posts, etc.)

4.8. Users should not publicly store DoS employees' personnel records

4.8.1. Examples of personnel records include compensation, rewards, reviews, or appraisals.

4.9. Users who violate or observe a user that is in violation of the Rules of Behavior will/should be reported to their local ISSO.

5. Non-Acceptable Uses

This policy identifies actions that should not be performed with SharePoint.

It is strictly prohibited to review, process, or modify PII, electronic protected health information or other delicate information while working within a SharePoint site. For more information on PII, please visit the Bureau of Administration's website regarding Privacy Matters: http://a.m.state.sbu/sites/gis/ips/privacy/default.aspx

SharePoint should not be used to post inappropriate documentation, announcements, lists, etc. that could be considered offensive by other site participants.

Cross enclave (OpenNet to ClassNet and vice versa) use of SharePoint is not supported.

Attachment 2

Privacy Act Statement

(Sample)

PRIVACY ACT STATEMENT

AUTHORITIES

The information provided in this form will be used by the Department of State and United States Secret Service to process your credential registration. All registration information is contained on a secure server which is designed to be accessed only by a limited number of employees.

PURPOSE

The information solicited on this form is required to process credential applications for approval to attend the 2009 Pittsburgh, Pennsylvania G-20 Summit. All required fields including Social Security Number for United States citizens are required to process credential applications. **This information will be used only by the United States Secret Service to provide the necessary validation prior to issuing credentials for this event**.

ROUTINE USES

The information on this form may be shared with the White House, Department of State and United States Secret Service:

Department of State Foreign Press Center
White House
All information provided will be collected and collated by the Department of State. The Foreign Press Center in collaboration with the White House is responsible for validation review and approval of applicants prior to submittal to the United States Secret Service. **These offices will not have access to any Personal Identifiable Information (PII)**.

United States Secret Service
The Secret Service is responsible for final validation and issuance of press credentials. The Secret Service will have access to all applicant information via a secure server. Based on the investigation results, information may be shared with the Department of Justice and other law enforcement agencies as needed.