Email the completed PIA to
PIAteam@state.gov

DOS-O365 PIA

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: Department of State – Office 365

(b) Bureau: Information Resource Management

(c) System acronym: DOS-O365

(d) iMatrix Asset ID Number: 260355

(e) Reason for performing PIA

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(a) Explanation of modification (if applicable) :

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

IA has completed the A&A assessment of DOS-O365 and we expect to receive the Authority to Operate (ATO) by June 1, 2017.

(c) Describe the purpose of the system:
DOS-O365 is a cloud-based Service (SaaS) solution that provides enterprise business productivity services and software. Licensed users have access to the services and software available via Office application integration. DOS-O365 includes services such as SharePoint Online, Dynamics Online, Power BI, Azure Information Protection, Skype for Business web conferencing, Exchange Online hosted e-mail for business, and

additional online storage with OneDrive for Business[1]. DOS-O365 includes the desktop version of the latest Office applications, which provide users a consistent experience across multiple computers and devices. These applications include Word, Excel, PowerPoint, OneNote, Outlook, Publisher, and Access.

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

Since users will have access to the variety of services and software available via Office application integration, and will employ them as tools in the course of their official business duties, IRM is unable to enumerate every possible use of DOS-O365. A few known/common examples are listed below.

Exchange Online E-mail uses names and e-mail addresses and sends, with the potential to collect in users' mailboxes, other subject matter that could contain other examples of PII. For instance, Human Resources may retrieve SSNs and other personal information through disseminated attachments; Bureau security offices request badge ID numbers from new hires; also temporary passwords (PINS) may be transmitted through the system. These are examples of how the DOS-O365 email system could be used, not necessarily how it is used.

SharePoint Online 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 Department 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

[1] Skype capacity is not part of the initial deployment and all IM usage will utilize the existing Lync system that is already in place.

- Biographic Information
- Mailing/Physical Addresses

Note: While IRM/OPS/SIO maintains DOS-O365 Enterprise system, we do not own the data or processes stored within the system. Information contained in DOS-O365is owned by the collecting office, bureau, or 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 DOS-O365 or by way of email will be dependent on the functional authority of the office collecting the information.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☐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, explain how the information is retrieved without a personal identifier.
The purpose of DOS-O365 is not to retrieve PII; it's a platform on which Department employees operate. Information covered by 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, and it is not possible to know all the ways DOS-O365 will be used.

In addition, the governing offices/bureaus collecting the PII, via services and software available via Office application integration, are responsible for ensuring they have appropriate SORN coverage and follow the appropriate procedures.

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

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 ☒No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

Data maintained by DOS-O365 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. Per the NARA directive emails classified as "Official – Privacy/PII" will be retained for seven years then deleted.

If yes provide:
- Schedule number (e.g., (XX-587-XX-XXX)): Click here to enter text.
- Length of time the information is retained in the system: Click here to enter text.
- Type of information retained in the system:
  Click here to enter text.

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 (people who are not U.S. Citizens or LPRs)

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

☒Yes ☐No

- If yes, under what authorization?

The governing authorities for collecting PII and/or SSNs by way of DOS-O365 system will be dependent on the functional authority of the office collecting the information.

(c) How is the information collected?

DOS-O365 serves as a repository of the information collected by the governing authorities. Emails are sent/received from a user's email client (Outlook). When the email is sent/received it's uploaded to the SMTP (Simple Mail Transfer Protocol) server as outgoing/incoming email. The SMTP server locates the recipient's email server (Exchange) and transfers the email to their inbox which resides there indefinitely until deleted.

For other aspects of DOS-O365, including SharePoint Online and OneDrive, 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 save the information from an Excel Online spreadsheet, Word Online document, or other file types that may be stored within a SharePoint Online repository or OneDrive.

(d) Where is the information housed?

☐ Department-owned equipment
☒ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

DOS-O365 will be hosted in the Microsoft Office 365 cloud.

(e) 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 DOS-O365. Likewise, email aspects of DOS-O365 only serve as a repository of information collected by governing authorities.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Maintaining current information is the responsibility of each bureau or office collecting the PII. Email aspects of DOS-O365 only serve as an information repository.

(g) Does the system use information from commercial sources? Is the information publicly available?

The uses of information collected in DOS-O365 vary by the mission of the office.

(h) Is notice provided to the individual prior to the collection of his or her information?

The owning office/bureau is responsible for notifying the individual prior to collecting their information.

(i) 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?

Click here to enter text.

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

The users' consent to use their PII is the responsibility of the owning office/bureau.

(j) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No (SharePoint & OneDrive aspects)

- If yes, how do individuals grant consent?

DOS-O365 is part of OpenNet and utilizes the single sign-on from OpenNet as the only method of access. The consent banner used at the OpenNet signon applies to DOS-O365. The provision of information is strictly voluntary. However, if a user declines to provide the information or consent to particular uses of the information, he/she may not be provided with the particular service he/she is requesting. SharePoint Online and OneDrive is typically used as a repository for information; therefore, consent is given at the initial point of collection.

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

Exchange Online is classified as Sensitive But Unclassified (SBU) due to the content of private information that users may include in their communications. Rules of Behavior have been established for end users to follow to ensure the laws and regulations governing the use of Exchange are being adhered to.

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.

Any office/bureau/post using the other aspects of DOS-O365 to collect, maintain, store or disseminate PII are responsible for completing the required privacy compliance documents.

5. Use of information

(a) What is/are the intended use(s) for the information?

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 and OneDrive:

- 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?
Yes. The purposes listed above are why DOS-O365 will be used at the Department and what it is 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?
Click here to enter text.

(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.

Any internal and/or external sharing of information varies by the mission of the office and is within the scope of the Department's regulations.

Recipients of the e-mailed information include approved DOS government and contracting personnel, various federal agencies, U.S. citizens and non-U.S. persons.

SharePoint Online and OneDrive are collaboration tools – they are 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.

(b) What information will be shared?

Any sharing of information varies by the mission of the office and is within the scope of the Department's regulations.

(c) What is the purpose for sharing the information?

Information is shared to support DOS business requirements and varies by bureau/office.

SharePoint and OneDrive, among other DOS-O365 cloud applications, are collaboration tools – they are designed to facilitate information sharing within the Department of State.

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

The way information is shared varies by bureau/office. The email aspects of DOS-O365 information to be shared are transmitted via a secure email gateway.

The DOS-O365 SharePoint Online and OneDrive information may be shared internally via the SharePoint application.

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

Safeguards related to sharing information in DOS-O365 are the responsibility of the collecting bureau/office.

(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 in DOS-O365. 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 maintained by aspects of DOS-O365 should contact the office/bureau that originally collected it.

Individuals wishing to access and amend Privacy Act covered information collected by SharePoint Online and OneDrive aspects of the DOS-O365 application should 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 https://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 at the U.S. Department of State Freedom of Information Act (FOIA) website at https://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. Individuals should contact 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?

The office/bureau collecting the PII provides the procedures or other mechanisms to correct users' information.

8. Security Controls

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

DOS-O365 information is housed on secure servers that are encrypted at rest and in transit by the FEDRAMP-approved Office 365 Cloud.

(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.

PII communicated through Department of State e-mail is accessible to cleared DOS direct hire and contractor employees. All access is enforced by user profiles according to the principle of the least privilege and the concept of separation of duties.

SharePoint Online and OneDrive aspects of DOS-O365: User roles are assigned by the bureau's site administrator to limit access to only those who have an official need to know. Additionally, individual users have the ability to share and limit content.

All DOS-O365: The Office 365 Security & Compliance Center lets you grant permissions to people who perform compliance tasks like device management, data loss prevention, eDiscovery, retention, and so on. These people can perform only the tasks to

which you explicitly grant them access. To access the Security & Compliance Center, users need to be an Office 365 global administrator or a member of one or more Security & Compliance Center role groups.

A user must be an Office 365 global admin, or a member of the Organization Management role group in the Security & Compliance Center, to grant these permissions. Role groups for the Security & Compliance Center might have similar names to the role groups in Exchange Online, but they're not the same. Role group memberships are not shared between Exchange Online and the Security & Compliance Center.

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

The Office 365 Security & Compliance Center can be used to search the unified audit log to view user and administrator activity in Office 365. The unified audit log allows ISSOs to search for the following types of user and admin activity in Office 365:

- User activity in SharePoint Online and OneDrive for Business
- User activity in Exchange Online (Exchange mailbox audit logging)
- Admin activity in SharePoint Online
- Admin activity in Azure Active Directory (the directory service for Office 365)
- Admin activity in Exchange Online (Exchange admin audit logging)
- User and admin activity in Power BI for Office 365

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

Both Government and Contracting staff are required to undergo annual PS800 Cybersecurity Awareness training and PA459 Protecting Personally Identifiable Information privacy training. If this requirement is not met, the individual will be locked out of the system.

(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.

Yes, data is encrypted per FIPS 140-2 guidelines.

(f) How were the security measures above influenced by the type of information collected?

Due to the nature and content of DOS business operations, system and security measures such as user authentication are in place to safeguard against unauthorized access or compromise to the system.

9. Data Access

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

Only Department-approved government employees or supporting contractors.

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

Access to system data is determined by security and support requirements. Access to collected data is role-based (2 types of user roles - Admistrative and End-User) on a need-to-know basis. The End-User only has access to content that they created or content that was shared with them. The Administrator has access to all admistrative features of DOS-O365 depending on the scope of their administration (example, there is an Exchange Administrator, Billing Administrator, SharePoint Administrator, User Management Admistrator, Security Compliance Administrator, etc). Permissions for Administrator roles adhere to the principle of least privilege and separation of duties so that within DOS-O365 admins only have access to the data they require to do their job. For example, SharePoint Administrators do not have access to Exchange data and are not able to view the same data as Compliance Administrators.

DOS-O365 management has assigned administrative roles for O365 role types based on existing permissions in place for the SharePoint and Exchange on premesis applications.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

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

No. Access to system data is restricted based on the employee's specific role.

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

Exchange Online E-mail, SharePoint Online, OneDrive, and Microsoft Office Online applications of DOS-O365: Access control is implemented via the secure network; authentication to the system is granted via Active Directory individual and group role membership. In addition, security tools are in place to proactively monitor subject system(s). Controls to prevent the misuse of data include mandatory cyber security training for all Department employees and contractors, privacy training, and the Department's Rules of Behavior for Protecting Personally Identifiable Information (PII).