PRIVACY IMPACT ASSESSMENT

Kiteworks PIA

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: March 2022
(b) Name of system: Kiteworks
(c) System acronym: N/A
(d) Bureau: Global Talent Management (GTM)
(e) iMatrix Asset ID Number: 320412
(f) Child systems (if applicable) and iMatrix Asset ID Number:
(g) Reason for performing PIA:

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

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

Kiteworks is a secure file transfer tool that enables users to send and receive encrypted information to/from Department of State (State) employees and external partners and share content via secure folders for secure document collaboration. All activity is encrypted and logged, and the Kiteworks platform provides insight of all content movement and user activity whether internal or external, whether desktop or mobile.

Kiteworks allows application administrators to provision user access easily and quickly to the system to allow secure exchange of data.

The Bureau of Global Talent Management (GTM) utilizes Kiteworks to allow for the secure exchange of files and documents related to Electronic Official Personnel File (eOPF) and employee/family member/intern related shared service requests.

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

The files and documents exchanged via Kiteworks may contain multiple PII elements including the following:

- Social Security Number (SSN)
- Full Name
- Beneficiary Data
- Date of Birth
- Death Certificate
- Personal Email Address
- Personal Phone
- Personal Address
- Passport Number
- Financial Information (e.g., Military buy-back documentation, Voluntary Separation Incentive Payment, etc.)
- Citizenship
- Educational Information (e.g., resumes, transcripts, diplomas, training, certificates, etc.)
- Military Service
- Personal Employment
- Mother's Maiden Name
- Spouse/Cohabitant Name
- Spouse/Cohabitant SSN
- Family Member(s) Information
- Dependent's Information
- Legal Information (e.g., Divorce Decree, Name Change by court order, Garnishments, Power of Attorneys, Judgements, Court Orders (Child support), Bankruptcies)
- Business Email
- Business Phone
- Business Title
- Business Address

The list of documents that GTM intends to transfer via Kiteworks includes all of the Office of Personnel Management (OPM) eOPF Master Forms List (opm.gov) as well as numerous forms related to beneficiary/survivor requests.

(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 Secretary of State)
- 22 U.S.C 2651a (Organization of the Department of State)
- 22 U.S.C 2901 et seq. (Foreign Service Act of 1980)
- 22 U.S.C. 3921 (Management of the Foreign Service)
- 22 U.S.C 4041 (Administration of the Foreign Service Retirement and Disability System)
- 5 U.S.C. 301-302 (Management of the Department of State)
- Executive Order 9397, as amended (Numbering System for Federal Accounts Relating to Individual Persons)
- Executive Order 9830 (Amending the Civil Service Rules and Providing for Federal Personnel Administration)
- Executive Order 12107 (Relating to the Civil Service Commission and Labor-Management in the Federal Service)

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

☒Yes, provide:

- SORN Name and Number:
  Human Resources Records, State-31

  SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  July 19, 2013

- SORN Name and Number:
  Security Records, State-36

  SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  June 15, 2018

☐No, explain how the information is retrieved without a personal identifier.

(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 Office 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.)

Kiteworks does not retain any documents, the documents transferred are always maintained by the owning system and/or gaining system, which have the retention policies.

If yes provide (Consolidate as much as possible):

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

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) On what other entities above is PII maintained in the system?

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☐ Other
☐ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No ☐N/A

- If yes, under what authorization?

Authorization for the Department of State to perform SSN collection comes from the following:

- 26 CFR 301.6109, Taxpayer identification
- Executive Order 9397, Federal employment
- 20 CFR 10.100, Federal Workers' Compensation

(d) How is the PII collected?

GTM utilizes Kiteworks for the secure and efficient exchange of forms, documents, spreadsheets, and files that contain PII. Kiteworks will never be the original collection source for PII. Instead, approved and authenticated users upload/download documents/spreadsheets/files containing PII via Kiteworks (web form or Outlook Plugin) once requested by an individual or other federal agency via email or phone. The Talent Services (TS) and Records and Information Management Divisions (RIM) within GTM will review and approve requests before creating a user account for the individual to upload the file. TS and RIM can also initiate a file request with individuals or other federal agencies as needed.

GTM/Talent Services (TS) estimates that approximately 350 unique OPM eOPF forms containing PII may be exchanged from/to GTM’s Integrated Personnel Management Systems (IPMS) via Kiteworks. This exchange may occur once or multiple times for each user, depending on necessary updates or corrections to each form. GTM/EX/Records and Information Management Division (RIM) will exchange Notifications of Personnel Action forms (SF-50s) from/to GTM’s Integrated Personnel Management Systems (IPMS) via Kiteworks. Other GTM divisions and/or offices may exchange spreadsheets and XML files containing PII with other federal agencies including the Government Accountability Office (GAO), the White House, the Department of Labor (DoL), and the Department of Defense (DoD).

(e) 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.

  Kiteworks is a FedRAMP-certified cloud, with an Authority to Operate (ATO) at the moderate impact level.

(f) What process is used to determine if the PII is accurate?

PII is uploaded to Kiteworks via forms/documents by individuals so there is no process used to determine if the PII is accurate within Kiteworks. The PII shared via Kiteworks is from authorized and authenticated users and generally via forms completed by the original source of PII.

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

Since PII is on forms/documents uploaded by individuals into Kiteworks, users may refer to the original documents/forms to determine if the information is current. The PII shared via Kiteworks is from authorized and authenticated users and generally via forms completed by the original source of PII.

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

Any information can be shared via Kiteworks, so long as the data type is moderate or low impact. However, GTM does not intend to utilize Kiteworks for exchange of information from commercial sources nor does it plan to use publicly available information

(i) How was the minimization of PII in the system considered?

All approved Kiteworks users will need to submit access requests and sign Rules of Behavior to ensure that they use Kiteworks only for PII exchange required to perform their duties. In addition, GTM/EX will ensure that files/documents exchanged via Kiteworks are only stored for the minimum time needed to ensure the transfer completes. As a business model within GTM, no documents/files containing PII will be accessible in Kiteworks for longer than 90 days. After 90 days, all documents/files delivered to/downloaded by the recipient will be deleted since Kiteworks is only approved for the transfer of documents and not storage.

5. Use of information

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

The PII exchanged via Kiteworks is used to perform human resource actions for employees, eligible family members, interns, annuitants, and prospective employees. The human resource functions include onboarding, determining benefit eligibility, requesting benefit changes, proving identity, etc.

GTM/EX will also utilize Kiteworks to securely provide ad-hoc reports containing PII to State bureaus. All ad-hoc report requests that contain PII are approved by the requestor's direct-hire, cleared supervisor and requests are logged by the GTM/EX/SOD leads who generate the reports.

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

Kiteworks, as a FedRAMP-certified cloud system, is approved for secure exchange of all data types up to the moderate impact level. The customer agency, GTM at State, determines the appropriate data exchanged via Kiteworks. As such, the use of PII by GTM is relevant to the purpose for which the system was designed.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

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

(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

(d) If the system will use test data, will it include real PII?

☐Yes ☒No ☐N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal: PII may be shared by GTM via Kiteworks with any post or bureau including the Bureau of Comptroller and Global Financial Services (CGFS), the Office of Medical Services (MED), the Bureau of Information Resource Management (IRM), the Office of Inspector General (OIG), and the Bureau of Administration (A Bureau).

External: PII may be shared by GTM via Kiteworks with the Office of Management and Budget (OMB), the Government Accountability Office (GAO), the Department of Labor (DoL), the Department of Homeland Security (DHS), the Department of Defense (DoD), and other external government agencies. PII may also be shared with separated employees, annuitants and/or their families, and their power of attorneys (POA). In addition, prospective interns may be approved to utilize Kiteworks to upload necessary documents containing PII.

(b) What information will be shared?

Internal: Various federal forms (e.g., DS5002, SF2809, W_4P, 13-22, SF 50) from the eOPF master list may be shared. In addition, all PII elements listed in 3d may be shared with the internal bureaus below based on business need, supervisor approval, and establishment of agreements, if necessary.

- Bureau of Comptroller and Global Financial Services (CGFS)
- Office of Medical Services (MED)
- Bureau of Information Resource Management (IRM)
- Office of Inspector General (OIG)

- Bureau of Administration (A Bureau)
- The Center for Analytics (M/SS/CfA)

External: Various federal forms (e.g., DS5002, SF2809, W_4P, 13-22, SF 50) may be shared. In addition, all PII elements listed in section 3d may be shared with the external partners listed below.

- Office of Management and Budget (OMB)
- Government Accountability Office (GAO)
- Department of Labor (DoL)
- Department of Homeland Security (DHS)
- Department of Defense (DoD)

Since GTM/EX/RIM is responsible for the transferal of an employees' Official Personnel Folder (OPF) to their gaining federal agency, the content of the OPF may include related PII (name, DOB, SSN, etc.), financial information, and benefit/beneficiary related PII. Financial forms are typically filed in the retirement folder (i.e., military/service buyback forms can disclose financial information) and the benefit/beneficiary related PII is housed in the administrative folder of the OPF.

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

Internal: PII and forms containing PII may be shared to facilitate human resource functions such as onboarding and benefit management, and to provide necessary reporting and cross-platform data sharing.

External: PII and forms containing PII may be shared to facilitate human resource functions such as onboarding, audits and reviews, benefit management, and OPF transferals (off boarding).

- Office of Management and Budget (OMB): On boarding and off boarding; reporting
- Government Accountability Office (GAO): Reporting and auditing
- Department of Labor (DoL): Workers Compensation, Unemployment Claims
- Department of Homeland Security (DHS): Secure Flight Program
- Department of Defense (DoD): Per Diem, Reporting, and On Boarding
- OPF Transfers to external Federal Agencies: Includes Personal, Financial and Benefit/Beneficiary related PII material.

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

Internal: PII and forms/documents/files containing PII can be uploaded to/downloaded from the Kiteworks web interface. OpenNet users may also utilize the approved Kiteworks Outlook plugin to send/receive PII and/or forms/documents/files containing PII.

External: PII and forms/documents/files containing PII can be uploaded to/downloaded from the Kiteworks web interface. External users are sent a secure email which contains a link to the file/folder in Kiteworks. On first use, the external user will be prompted to create a password and receive a one-time PIN via their registered email address.

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

Internal: Non-GTM Kiteworks users are required to submit an access request which must be approved by either a) their direct-hire supervisor, or b) the GTM ISSO or alternate ISSO. In addition, each non-GTM Kiteworks user must sign the Kiteworks Rules of Behavior and must have taken the FSI PII course (PA-318 Protecting Personally Identifiable Information). Non-GTM users who require the ability to upload or add users must also be approved by the GTM ISSO or Alternate ISSO. The GTM ISSO team performs audits of all user activity including user access creation, user role changes, and user upload/download activity.

External: External users must be approved by one of the GTM application administrators. The GTM ISSO team performs audits of all user activity including user access creation, user role changes, and user upload/download activity. User location is considered for external users, and any perceived unusual activity will be verified by the GTM ISSO team.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes, all PII exchanged via Kiteworks is collected by approved systems which have Privacy Act statements at the original point of collection.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

Kiteworks does not collect PII directly, but only transfers it from the original point of collection.

(c) What procedures allow record subjects to gain access to their information?

The original sources of the PII exchanged via Kiteworks are responsible for providing procedures for record subjects to gain access to their information.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

The original sources of the PII exchanged via Kiteworks are responsible for providing procedures for record subjects to correct inaccurate or erroneous information.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

The original sources of the PII exchanged via Kiteworks provide individuals notice of the procedures to correct their information.

8. Security Controls

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

Kiteworks is a FedRAMP-certified cloud secure document exchange platform. As such, security has been assessed by an approved third-party independent assessor (3PAO) and approved by the FedRAMP Program Management Office. Kiteworks is required to encrypt data at rest and in transit using federally approved (NIST 140-2) encryption products. The encryption keys for each customer instance are maintained by the customer, meaning that Kiteworks' staff do not have the ability to decrypt customer data and files. In addition, Kiteworks must conduct continuous monitoring activities which include scheduled vulnerability scans, penetration testing, code analysis, user access reviews and audits, personnel security procedures, incident response and handling, and configuration management. As a Kiteworks customer, GTM also drafts user access procedures which include mandatory 2-factor authentication, performs user activity audits, and reviews incident notices.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

All Kiteworks users have access to files/folders created/uploaded by them or shared with them by another user. Users cannot view the contents of files/folders that they have not uploaded or been granted explicit permissions to. In addition, the roles below provide additional permissions.

The standard Kiteworks roles include:

- **System Administrator** – System administrators are responsible for configuration, maintenance, and management of the GTM Kiteworks instance. System administrators can create any role and view a list of all files/folders created by any user, as well as change ownership of files/folders. Changing file/folder ownership grants the new owner full access to the files/folders. System administrators can only access files/folders they upload or have a user upload for their receipt.
- **Chief Information Security Officer (CISO)–** Chief Information Security Officers are responsible for the security of the system. They have a read-only role with access to audit and usage logs but no access to individual files/folders except any files they upload or files they request.
- **Application Administrator** – Operational staff responsible for configuring application settings. Application administrators can create another application administrator, helpdesk administrator, power user, and standard user accounts. They also can set or change application settings such as timeout value, maximum file size, etc. Application administrators can only access files/folders they upload or have a user upload for their receipt.
- **Help Desk Administrator** – Operational staff responsible for configuring the file/folder permissions and adding regular and power users. Help desk administrators can create another help desk administrator, power user, and standard user accounts. They can also reset user passwords. Help Desk administrators can only access files/folders they upload or have a user upload for their receipt.
- **Power User** – Power users create folders for collaboration within Kiteworks and control who has access to the folders. Power Users have access to files that they upload, and any file shared by another Kiteworks user.
- **User** –Users can receive or upload files and exchange files with internal and external users. They have access to files that they upload, and any file shared by another Kiteworks user.

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

All GTM Kiteworks users are required to submit an access request approved by their supervisor. Each GTM Kiteworks user must also sign the Kiteworks Rules of Behavior and complete PA-318 Protecting Personally Identifiable Information. Non-GTM users have the same requirements but must also be approved by the GTM ISSO or alternate ISSO if the user requires upload or add user capability. The GTM ISSO team performs audits of all user activity including user access creation, user role changes, and user upload/download activity.

External (non-Department of State) users are also required to submit an access request approved by one of the GTM application administrators. The GTM ISSO team performs audits of all user activity including user access creation, user role changes, and user upload/download activity. User location is taken into account for external users, and any perceived unusual activity is verified by the GTM ISSO team.

Kiteworks employees do not have access to customer instances. Kiteworks has procedures that allow customer system administrators to provide access to Kiteworks staff to troubleshoot issues.

(d) How is access to data in the system determined for each role identified above?

Specific roles in Kiteworks are determined by business need. All Kiteworks user requests for State employees/contractors must be approved by a direct-hire supervisor. Non-State users may be approved by State Kiteworks Application Administrators or a member of the GTM ISSO team. Access to specific PII is based on user roles within State or from external agencies/vendors.

- **System Administrator** – Employees of the GTM/EX Helpdesk and Operations and Architecture branch are approved for this role by the GTM ISSO, GTM alternate ISSO, GTM/EX/ESD Chief, or GTM/EX/OTS Chief Technology Officer.
- **CISO** –Access to this role is approved by the GTM ISSO.
- **Application Administrator** – Access to this role is approved by the GTM ISSO, GTM alternate ISSO, GTM/EX/ESD Chief, or GTM/EX/OTS Chief Technology Officer.
- **Help Desk Administrator** –Access to this role is approved by the GTM ISSO, GTM alternate ISSO, GTM/EX/ESD Chief, or GTM/EX/OTS Chief Technology Officer.
- **Power User** – Must be a Division Chief or Division Chief or delegated by a Division Chief and approved by the GTM ISSO or Alt ISSO.
- **User** – Based on business need, approved by a power user or GTM ISSO or alternate ISSO.

System access is based on need to know. The GTM Kiteworks system, application, and helpdesk administrators will be approved by the system owner (the GTM/EX/CTO) or the GTM ISSO or alternate ISSO. Power users will be approved by the user’s direct hire supervisor and GTM ISSO/alternate ISSO. All other users will be approved by the application administrators or power users and will not have the ability to add users or change the default length of time that files may be stored in Kiteworks. Any external users with elevated access will be approved by the system owner and GTM ISSO/alternate ISSO. Kiteworks can disable accounts based on inactivity, and GTM administrators will ensure that all accounts are set to be automatically disabled if inactive for 60 days.

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

Kiteworks logs all user access changes and user upload/download activity, to include location (IP Address) of user activity. These logs are accessible to users in the CISO role and cannot be modified by any users.

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

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

There is no role-based training for this system; however, all Department of State users are required to take biennial PII course, PA318 Protecting Personally Identifiable Information, and annual Cyber security Awareness course, PS800, which has a privacy component. Access to the Department's intranet is disabled if users do not take and pass PS800 course annually. The GTM ISSO will ensure that all internal users have taken the Department's PII course. Any external user granted elevated access will sign a Rules of Behavior which will be kept on file and updated annually by the GTM ISSO/Alt ISSO.