PRIVACY IMPACT ASSESSMENT

Enterprise Collaboration - Slack (EC-Slack)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA:

08/2021

(b) Name of system:

Enterprise Collaboration - Slack

(c) System acronym:

EC-Slack

(d) Bureau:

R/PPR

(e) iMatrix Asset ID Number:

151209

(f) Child systems (if applicable) iMatrix Asset ID Number:

N/A

(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):

EC-Slack was formerly part of the PD Suite (iMatrix #272834) system managed by Global Public Affairs and was named PD Chat (iMatrix #151209) at that time. As of November 2019, R/PPR has taken over management of Slack. PD Chat has been transferred to R/PPR's State Collaboration Tools investment in iMatrix, using the same ID number. This PIA updates ownership of the system and separates it from PD Collaboration (iMatrix #106241) and PD Monitor (iMatrix #272913), the other systems that comprised PD Suite.

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:

Enterprise Collaboration-Slack (EC-Slack) is a Department of State program and Software as a Service (SaaS) solution created to provide industry-standard collaboration and information sharing on a common cloud platform. EC-Slack is used widely within R/PPR and is offered as a shared service to the Bureaus of Global Public Affairs (GPA) and Educational and Cultural Affairs (ECA), and Embassies, Posts and Missions under Chief of Mission Authority as a direct response to the growing need for a more secure, coordinated, and cost-efficient overseas communication. EC-Slack is organized into Workspaces by topic and job function membership. EC-Slack enables State Department personnel around the globe access to web-based communication services to support the business of the agency, collaboration with partners, and anytime, anywhere access to information.

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

The EC-Slack USG user/member profile includes the following type of information:

- First Name (mandatory)
- Last Name (mandatory)
- Business Phone Number (voluntary)
- Government Issued Mobile Number (voluntary)

- Business Email address (mandatory)
- Profile Photo (voluntary)
- Slack Username (voluntary)

The EC-Slack non-USG user/member profile includes the following type of information:

- First Name (mandatory)
- Last Name (mandatory)
- Business Phone Number (voluntary)
- Government Issued Mobile Number (voluntary)
- Business Email address (mandatory for .org or .edu business emails)
- Profile Photo (voluntary)
- Slack Username (voluntary)

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

- 5 U.S.C. 301, Management of Executive Agencies
- 22 U.S.C. 2651a, Organization of the Department of State

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

☒ Yes, provide:
- SORN Name and Number: STATE-56 Network User Account Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): December 12, 2017

☐ 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.)

If yes provide (Consolidate as much as possible):
- Schedule number (e.g., (XX-587-XX-XXX)):
  1) A-03-003-11 System Access Records
  2) A-03-005-04 Transitory Records

- Disposition Authority Number:
  1) DAA-GRS2013-0006-0003 (GRS 3.2., item 030)
  2) DAA-GRS-2017-0003-0001 (GRS 5.2, item 010)

- Length of time the information is retained in the system:
  1) Temporary. Destroy when business use ceases.
  2) Temporary. Destroy when no longer needed for business use, or according to agency predetermined time period or business rule. (Supersedes GRS 23, item 6a; GRS 23, item 6b(1); GRS 23, item 6b(2); and GRS 23, item 7)

- Type of information retained in the system:
  For access purposes, member names and work/organizational/school-related email addresses. Information contained in individual posts in Slack channels or direct messages is required only in the short term, e.g. less than 180 days, and pertains to routine business projects and programs across different work streams, typically arranged by topic or office.

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. citizens with guest accounts who have limited access to the system; these guests are non-Department employees who are conducting business in collaboration with Department employees)

☒ 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?

(d) How is the PII collected?

The information collected for this system is obtained directly from the user via a System Access Request Form (SARF) (https://forms.gle/PSs8G89jHz4ezxwv6). To register for an account, the user must provide their name and business email address. Once the user logs in, they navigate to their member profile and can optionally fill in additional fields about themselves, such as those listed in 3(d).

(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.

All EC-Slack data is hosted by Slack, Inc., whose system resides on Amazon Web Services (AWS), US-East. AWS is also FEDRAMP-certified.

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

Accuracy of the information is the responsibility of the user. The PII that is entered into the system is obtained directly from the user during the registration process. Users enter their own PII in their member profile, thus it is presumed to accurately reflect the user's name, email address, phone number, and other work-related information the user chooses to provide.

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

Yes, the information is current. Responsibility to keep information current falls solely on the user. Users can log into the system any time to ensure that profile information is current. Users are also reminded to update their profile information on a quarterly basis, or when they change jobs or locations.

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

The system does not use information from commercial sources. Some of the information is publicly available. The system has an RSS feed application integration that collects information from public news sources. The feeds provide content for specific public channels that are related to the type of news articles included in the feed. For example, the Bureau of Educational and Cultural Affairs gathers public news articles about exchange programs via RSS feed, and these stories are posted in the *#eca-highlightstories* public channel.

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

The minimum amount of information required to create an account was defined for collection by the system based on its requirements. Users are required to provide their name and a professional, organizational, or school-issued email address in order to have an account in Slack. No other information is mandatory. Slack is monitored by Cisco Cloudlock (Public Diplomacy Monitor), currently managed by GPA. Cloudlock identifies sensitive information like SSN and alerts system administrators that the data is present and to take corrective action. The amount of PII collected is minimized to the extent needed to fulfill the system's function.

5. Use of information

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

The system's intended use, as described in 3(c), is for a more secure, coordinated, and cost-efficient communication and collaboration between State Department personnel around the globe. PII collected, except for name and email for account creation, is voluntary and visible only to other Slack users. They can use this information to learn more about colleagues or contact them directly.

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

Yes. EC-Slack is designed to foster collaboration and communication amongst the members of the Department and across bureaus. The PII collected is necessary and kept solely so that the system can perform the functions that it was designed for. No collateral uses exist for the PII collected by the system.

(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:

Information will be shared internally with the Bureau of Information Resource Management's State Enterprise-Identity, Credential and Account Management (IRM SE-ICAM) team.

External:
No information from Slack is shared with external entities.

(b) What information will be shared?

Internal:
Name and email address are shared with Okta, the Department's State Enterprise-Identity, Credential, and Access Management (SE-ICAM) solution.

Slack users that have a state.gov account will automatically have an Enterprise Okta account.

Approved external Slack users (without a state.gov account) are assigned a non-Enterprise Okta account. The individual's name and email address are required for that purpose.

External:
No information from Slack is shared with external entities.

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

Internal:
The purpose of sharing the information with Okta is to authenticate users' access to the Slack application.

The SE-ICAM program covers the identity, credentialing, and access management functions. The SE-ICAM team uses the Slack account information for credentialing and manages all Okta accounts for both internal Department employees who have Azure Active Directory accounts, as well as non-Department users who have been approved by a Department employee to have access to Slack.

External:
No information from Slack is shared with external entities.

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

Internal:
Okta, the Department's standard authoritative authentication enterprise service for cloud systems, connects to Slack via a SCIM API (System for Cross-domain Identity Management Application Programming Interface) connection. This connection manages the basic identity credentials (business name, email) provided by IRM.

External:
No information from Slack is shared with external entities.

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

Internal:
Only designated personnel, Slack and Okta administrators with signed admin forms, have access to the information. The data is read-only, as it cannot be edited through the API when passed between systems. The SE-ICAM team and the EC-Slack system owner completed a standard requirements agreement that is required for all third-party applications that use the Okta identity management system. The standard requirements agreement includes the safeguards in place for this sharing arrangement which are controlled via direct API connection handled between Slack and Okta. Those safeguards include Single Sign-On (SSO) and Multi-factor Authentication (MFA) requirements for users and admins of both Slack and Okta, and read-only data sharing limited to required admin accounts only.

External:
No information from Slack is shared with external entities.

7. Redress and Notification

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

Yes, the SARF has a Privacy Act statement that appears on the first page. This PAS lists the authorities the Department has that allow it to collect this information, why the information is being collected, with whom the information will be shared, and whether the information is mandatory. It also provides the applicant with information about the System of Records Notice (SORN) that governs the collection of this information where the applicant can learn more about how their PII will be utilized.

(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?

Individuals must accept the EC-Slack SARF's terms before they will be granted a user account. Without express consent, an individual cannot access the system.

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

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

Individuals have full control over their own profile by logging in with their Okta credentials.

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

☒Yes ☐No

If yes, explain the procedures.

Each EC-Slack user can access and correct his or her own information once they log into their account and enter their profile. Users can modify their own profile information at any time. Users can also ask for assistance modifying their profile from other users, primarily through the public tech support channel called #tech-ambassadors, which can be found through the general Slack search function, or with the Channel Browser tool. Users can also get instructions directly from the EC-Slack administrators. Users can seek help through Slack's built-in help function, located in the Slack menu bar at the top of every page throughout the platform, or they can get instructions directly from the EC-Slack administrators through the email RCTO@state.gov.

If no, explain why not.

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

All users receive a welcome email upon account creation, after filling out the access request form. The welcome email includes a basic platform introduction, along with instructions on how to update their profile and join channels like #tech-ambassadors. The Slack administrator reminds users to update their profiles quarterly, via notice to multiple general-use channels, particularly #tech-ambassadors and #global-general. All new users, except guests, are put into #global-general when their account is created. This default channel provides major platform updates from Slack administrative staff to all Slack members.

8. Security Controls

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

Slack leverages AWS' services to encrypt customer and message data at rest, stored in MySQL database servers that run on disks using NVMe instance storage. This storage is encrypted using an XTS-AES-256 block cipher implemented in a FIPS 140-2 validated hardware module on the instance, provided by AWS.

(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).

Slack Role	**Min Clearance level**	**Foreign National**	**Description**
Workspace Owner	Secret	Not Allowed	Full administrator with access to API (Application Programming Interface) controls and SSO (Single Sign On) configuration
Guest - "non-USG User"	Uncleared	Allowed	External users granted limited access to specific channels and direct messages.
Workspace Admin	Secret	Conditionally Allowed	Administrators that can manage users and channels, as well as most configuration settings
Workspace Primary Owner	Secret	Not Allowed	Full Administrator with access to billing and data compliance export functionality. Only this person can delete the workspace or transfer primary ownership to someone else.
Full Member - "DoS User"	Secret	Allowed	Normal users enrolled via SSO (Single Sign On). Some staff have MRPT (Moderate Risk Public Trust).

(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.

Access to EC-Slack resources, services and information is restricted to personnel who are approved by a State Department supervisor or contracting officer representative, or to guest users who have been invited to join a channel by a Department employee. EC-Slack administrators must complete and have a supervisor approve the SE-ICAM System Access Request Form (SARF) to be permitted to have administrator access to Okta. EC-Slack implements a single sign on (SSO) system to manage and control access to Slack cloud services. The SE-ICAM team does not have EC-Slack accounts and cannot access any user information beyond name and email address, as required for Okta authentication. Role-based access control (RBAC) is implemented for least privilege and segregation of duties. Private channels can be accessed only by the user that created them and other users that are specifically invited to join the channel. Direct messages can only be viewed by the users communicating in the message. Guest users may only access the channel(s) they are a member of.

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

The roles listed in the table above are defined by Slack for any Workspace - each Workspace will feature a Workspace Primary Owner, one or more Workspace Owners, one or more Workspace Administrators, Full Members, and if an organization chooses, Single- or Multi-Channel Guests. The type of actions each of these roles can perform and the data each role has access to are defined by Slack and R/PPR cannot change those features or types of access but does control which individuals are assigned to each type of role.

Slack Role	Available PII
Workspace Owner	Can view and download user list containing only: First Name, Last Name and Business Email.
Guest - "non-USG User"	Guests can only view the Profiles of the other users they interact with in shared channels.
Workspace Admin	Can view and download user list containing only: First Name, Last Name and Business Email.
Workspace Primary Owner	Can view and download user list containing only: First Name, Last Name and Business Email.
Full Member - "DoS User"	Members can view the Profiles of all users.

Workspace Primary Owner – The R/PPR senior executive selects the employee that fulfills this role, which is the equivalent of the Business Sponsor/Owner of the EC-Slack Workspace. The person in this role must be a direct-hire Department employee. This role is the only Slack role that has the ability to delete the entire Workspace or transfer ownership to another individual.

Workspace Owner(s) - The Workspace Primary Owner determines who will perform as a Workspace Owner. Workspace Owners must be direct-hire department employees. They have full data and administrative access to EC-Slack, but typically do not perform day-to-day administration of the Workspace.

Workspace Admin(s) - The Workspace Primary Owner solely or in collaboration with the other Workspace Owner(s) assign individuals to the Admin role. Admins may be direct-hire or contract employees that have a background in and skills managing IT systems, or may be trained to administer EC-Slack. Workspace Admins manage access to EC-Slack for all full members and single- and multi-channel guests. They work with the IRM SE-ICAM team to ensure all user types log into EC-Slack with the Okta identity management system. Admins do not have access to private channels or direct messages that they themselves do not participate in. They retain elevated privileges to perform administrative tasks until they change job functions or leave R/PPR.

Full Members – this is the default role assigned to the majority of EC-Slack users, and is based on the information the individual enters into the SARF. Only Department direct-hire employees, contractors, REAs, and LES may be full members.

Single-channel or Multi-channel Guests - Individuals not employed by the Department but working in direct partnership may be invited to EC-Slack as one of these two types of Guests, depending on their interactions with Department programs and need to know. Guest access is limited to one or a few channels, can only participate in those channels, and do not have access to user profiles outside the channels they belong to. Guest accounts must be re-validated every 60 days by the office that sponsors the guest's membership.

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

EC-Slack is monitored through the use of auditing and logging tools provided directly by the Slack platform, as required for its FedRAMP authorization. Effective monitoring and the ability to track user and administrator activities are critical in preventing, detecting, analyzing, and minimizing the impact of a data compromise. Auditable events include:

- Successful and unsuccessful account logon events
- Privileged functions, e.g. channel deletion
- Account management events – creation, deletion, changes in role
- System events, e.g. software upgrade, hardware failure.

Only Workspace Owners and Admins have access to the audit logs, which are stored by Slack for the life of the Workspace.

The Cloudlock Cloud Access Security Broker also monitors EC-Slack. Cloudlock provides Data Loss Prevention software that monitors EC-Slack for various types of PII such as social security or passport numbers. Cloudlock is also FedRAMP-authorized.

(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.

All authorized Department users identified in 8(b) that have access to the PII in this system must complete the mandatory annual security training PS800: Cyber Security Awareness and the biennial privacy training PA318: Protecting Personally Identifiable Information. The Cyber Security Awareness training has a privacy component and users must complete it every year in order to maintain OpenNet access.