PRIVACY IMPACT ASSESSMENT

Foreign Affairs Network (FAN)

1. Contact Information

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

2. System Information

(a) **Date of completion of this PIA**: January 2021
(b) **Name of system**: Foreign Affairs Network
(c) **System acronym**: FAN
(d) **Bureau**: IRM/OPS/CPMO
(e) **iMatrix Asset ID Number**: 212914
(f) **Child systems (if applicable) iMatrix Asset ID Number**: Not Applicable
(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:

FAN is a portfolio of secure, cloud-based services that enable a highly mobile, productive, and collaborative workforce spanning the Department of State and its foreign affairs partners. The FAN system provides the Department of State an environment to support the agility needed to rapidly select, deploy, integrate and secure cloud-based digital productivity tools for its global workforce. FAN also provides a cloud-based infrastructure to support Department of State custom applications built upon cloud services provided and managed by the FAN program.

FAN provides Chiefs of Mission overseas the ability to reach all of their staff, regardless of agency. FAN connects Department of State personnel with other government agency personnel at embassies/posts/missions to allow appropriate access to essential mission information that needs to be shared for effective coordination and collaboration. The FAN system provides features to enable Department of State personnel to securely collaborate and share information with other federal government agency personnel, including contracting personnel, in support of the mission. Additionally, FAN provides the means to enable family members overseas to access post resources like management and security notices.

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

IRM/OPS/CPMO requires the following from non-enterprise users (users with no OpenNet account) of FAN to uniquely identify them for access to the FAN system: name, organization, business phone number, business email address, employee type, job title, security clearance status, and business address.

IRM/OPS/CPMO requires the following from enterprise users (users with an OpenNet account) of FAN: name and business e-mail address.

Users are Department of State employees (and authorized family members), contractors, and other government agency foreign affairs partner personnel with a need to collaborate and that are approved access to FAN by Chiefs of Mission.

FAN is a general support system providing an environment for users to store and process Sensitive But Unclassified (SBU) information to include Consular, Financial, Medical, and Personnel (HR) data. While IRM/OPS/CPMO has built FAN to provide security protections to support these data types, FAN users are required to coordinate and ensure approval is granted by the Privacy Office for any PII collections stored in FAN by completing the FAN-Use PIA template. This PIA only covers the PII collected by FAN for user account creation.

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

5 U.S.C. 301; 44 U.S.C. 3544; and 44 U.S.C. 3541.

(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)): A-03-003-11
- Disposition Authority Number: DAA-GRS-2013-0006-0003 (GRS 3.2, item 030)
- Length of time the information is retained in the system: Temporary. Destroy when business use ceases.
- Type of information retained in the system: System Access Records.

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 (for this system, eligible family members are considered employees, as their access to FAN is solely due to their relationship to an employee.)
☐ 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?

IRM/OPS/CPMO uses the DS-7771 form and the FAN General Account Creation Request Form, via ServiceNow, to collect user information for account authorization. The ServiceNow form was created to replace the DS-7771 which is planned for retirement in early 2021. The myData system is used to present this form to users, store the data, and provide workflow for approval processing. Currently, a PDF-fillable version of the DS-7771 form is also used for personnel that do not have access to myData. Users are responsible for protecting the information in the PDF-fillable DS-7771 form until submitted to IRM/OPS/CPMO FAN program via OpenNet e-mail. Once the DS-7771 form is retired, a supervisor or colleague with access to the FAN General Account Creation Request Form will submit it on behalf of personnel that do not have access to ServiceNow.

(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.

Information processed in FAN is stored in the FAN Google G Suite cloud service. Google G Suite, and its underlying Google Common Infrastructure (GCI) are FedRAMP-certified cloud services under the label Google Services. Google implements NIST approved encryption modules to ensure protection of data at rest and in transit. Google G Suite is available in all Google Datacenters included within the Google Services security authorization boundary.

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

All users who request access to FAN must fill out a DS-7771 form or the FAN General Account Creation Request Form via ServiceNow. FAN uses Okta for account identity and authorization. For users with an existing OpenNet account, Okta verifies the user's identity through OpenNet Active Directory (AD). For FAN users that do not have an OpenNet account, IRM/OPS/CPMO relies on Department of State supervisors, Information Management Officers (IMO), Regional Security Officers (RSO) and/or Bureau Security Officers (BSO) that are included in the approval workflow process for review and accuracy of the information submitted in each request for a FAN account. Upon receipt of request for a FAN account, IRM/OPS/CPMO validates that each request has been properly completed, routed and approved by the necessary personnel.

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

By leveraging existing Department myData services, IRM/OPS/CPMO ensures user information is current. All users are required to maintain their personal information in the Department myProfile system which is used by the myData service that supports FAN account creation. After account creation, an annual review process is used to ensure information remains accurate. IMOs at post and bureau/office representatives and supervisors participate in the review with the FAN System Owner. Changes determined through these reviews are implemented accordingly.

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

No, the system does not use information from commercial sources or publicly available information.

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

For FAN enterprise users who already have an OpenNet account, only user name and OpenNet email address is required. When creating the FAN account, the OpenNet email address is used by Okta (DOS Enterprise Identity Manager) to automatically leverage existing user information from OpenNet Active Directory in order to create the user's FAN account. For all non-enterprise users, full name, business email address, employee type, job title, business phone number, organization and security clearance status is required. IRM/OPS/CPMO eliminated the need to collect the specific location, badge numbers and citizenship status of both enterprise and non-enterprise users.

5. Use of information

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

The information collected by IRM/OPS/CPMO for FAN user account creation is used to grant and manage access to the FAN system based on organization affiliation, role, and need to know for access to information and system privileges.

(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.

(c) Does the system analyze the PII stored in 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: Not Applicable. No information is provided to another entity or extracted by another system.
External: External sharing of PII is not authorized on FAN.

(b) What information will be shared?

Internal: None.
External: None.

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

Internal: Not Applicable.
External: Not Applicable

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

Internal: Not Applicable.
External: Not Applicable.

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

Internal: Not Applicable.

External: Though external sharing does not occur, FAN uses CloudLock to detect and block the external sharing of PII.

7. Redress and Notification

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

Yes. The individual is informed of the collection of PII during the FAN account request process. Both the DS-7771 and FAN General Account Creation Request Form via ServiceNow contain a Privacy Act statement which informs the user of the purpose and use of their PII.

(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?

If the user does not grant consent, their request for access to the FAN system will not be approved and user access is denied.

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

Individuals who wish to gain access to or amend their records must send an email to ITServiceCenter@state.gov to reach the Bureau of Information Resource Management. Individuals should indicate in the subject line “Request personal information for FAN Account” and include in the body of the message the FAN user account email address along with the business telephone number where the individual can be reached during normal business hours.

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

☒Yes ☐No
If yes, explain the procedures.

Individuals who wish to gain access to or amend their records should send an email to ITServiceCenter@state.gov to reach the Bureau of Information Resource Management. Individuals should indicate in the subject line “Request update of personal information for FAN Account” and include in the body of the message the FAN user account email address along with the business telephone number where the individual can be reached during normal business hours.

If no, explain why not.

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

Individuals requesting access to the FAN system are made aware of the redress procedures via the DS-7771 and ServiceNow form which all users must sign to obtain access to the FAN system.

8. Security Controls

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

- User account creation requests, in the form of the DS-7771 form and the FAN General Account Creation Request Form, via ServiceNow, are stored and protected in the Department myData system which resides on the OpenNet network.
- All requests for access to FAN must be approved by a supervisor and FAN System Manager. All users must sign the FAN Access Agreement and Rules of Behavior, which describe the rules for use of the system and the user's responsibilities as it pertains to privacy and security.
- Google G Suite – Google encrypts all data (in transit and at rest) stored in Google G Suite with FIPS 140-2 approved encryption module.

(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).

- **Users –** Access to this system is restricted to cleared Department of State (DoS) direct hire and eligible family members and contractor employees. FAN relies on DoS to screen employees and contractor personnel as part of onboarding process and for changes to duty assignments to ensure that 12-FAH-10 H-282.2 criteria are met based on the individual, work location (domestic or abroad), and information access requirements. Users have access to PII that is stored in the FAN user directory which includes a user's name, title, business email address, business telephone number and office.
- **Privileged Users –** System administrators (Help Desk Admin, Services Admin, Android Admin, Groups Admin, Super Admin, User Management Admin, ExecTech Support Admin, FAN Digital Signage Admin, FAN Local Admin and FAN Enterprise Support) create accounts, and administer and manage the system. System administrators have logon identifications associated with their name that allows for user auditing. System administrators have access to username, business email, work location, employee type, manager name and email address and work and personal phone numbers. The FAN System Owner must authorize personnel which have a need for permissions or privileges that require access to user account PII.

(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.

The FAN system has defined roles for users of the system. The FAN System Owner must authorize personnel which have a need for permissions or privileges that require access to user account PII. These privileged accounts are monitored continuously and reviewed annually.

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

- **Users –** User only have access to their information and other information which they are granted access to based on their organizational requirements and the determination of the information owner. All users have access to PII that is stored in the FAN user directory which includes a user's name, title, business email address, business telephone number and office.
- **Privileged Users –** System administrators are responsible for granting and removing access to the system for all users. As such, system administrators will maintain full administrative access to the system and have access to the PII identified above by default. Access to the system is revoked once the privileged user terminates or is reassigned to a different position.

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

FAN uses Cisco CloudLock to monitor FAN domains and is configured with rules and policies to detect security violations, malicious behavior, insider threats and breaches. CloudLock is also configured with rules and policies to detect any attempt at external sharing of PII.

All access and activity on FAN and its cloud services is audited. All audit data are correlated and reviewed by FAN security operations personnel and State Department Diplomatic Security to detect unauthorized access and misuse.

(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.

Department personnel including contractors are required to take the mandatory PII Training, PA318 Protecting Personally Identifiable Information biennially, and DOS PS800 Cyber Security Awareness Training annually.