Foreign Affairs Network (FAN)

1. Contact Information

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

2. System Information

(a) Name of system: Foreign Affairs Network

(b) Bureau: Information Resource Management (IRM/FO/OII)

(c) System acronym: FAN

(d) iMatrix Asset ID Number: 212914

(e) Reason for performing PIA: Click here to enter text.

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

(f) Explanation of modification (if applicable): The PII required to operate FAN is limited to user account identification information. However, the FAN is used to support broad processing needs of Department of State personnel. To accommodate this, the FAN system was modified to provide security protection to all PII information types. Processes have been put into place to require all FAN users to obtain approval from the Privacy Office prior to processing PII information in FAN.

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?
The Department of State Chief Information Officer (CIO) granted an Authority to Operate (ATO) for FAN in August 2017. The FAN system is in the continuous monitoring phase of the NIST Risk Management Framework (RMF).

(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 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/FO requires the name, organization, badge number, phone number, email address and business address of each user of the system to uniquely identify users for access to the FAN system. 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/FO 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.

(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)?

☒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): 12/12/2017

☐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 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 .)

If yes provide:
- Schedule number (e.g., (XX-587-XX-XXX)): A-03-003-11
- 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) - Locally Employed Staff (LE Staff) and 3rd Country National (TCN)

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

☐Yes ☒No (SSNs are not collected)

- If yes, under what authorization?
Click here to enter text.

(c) How is the information collected?
IRM/FO uses the DS-7771 form to collect user information for account authorization. The Department myData system is used to present this form to users, store the data, and provide workflow for approval processing. A PDF-fillable version of this 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/FO FAN program via OpenNet e-mail.

(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.
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.

(e) What process is used to determine if the information is accurate?
For FAN users that already have a Department OpenNet system account, IRM/FO relies on existing OpenNet user account processing for information accuracy. For FAN users that do not have an OpenNet system account, IRM/FO 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 FAN account, IRM/FO validates that each request has been properly completed, routed and approved by the necessary personnel.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
By leveraging existing Department myData services, IRM/FO 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.

(g) 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.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes. The individual is informed of the collection during the FAN account request process. The DS-7771 form used by FAN to support access requests contains a Privacy Act Statement which informs the user of the purpose and use of the user's personal 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?
- If no, why are individuals not allowed to provide consent?
If user does not wish to grant consent, the request for access to the FAN system will not be approved and user access is denied.

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

In order to limit the PII collected in FAN, the information necessary to create a user account is limited to only what is necessary to validate identity and to ensure proper routing of credentials.

5. Use of information

(a) What is/are the intended use(s) for the information?
The information collected by IRM/FO for FAN system account approval 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 information relevant to the purpose for which the system was designed or for which it is being designed?
Yes.

(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?
Click here to enter text.

(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.
Security event and audit data, which contain user identity along with system access and activity, is shared internally with the Bureau of Diplomatic Security in accordance with State policy for security monitoring 12 FAM 500.

(b) What information will be shared?
User access and activity audit logs.

(c) What is the purpose for sharing the information?
The information is shared for the purpose of monitoring the system for cybersecurity incidents and user policy violations.

(d) The information to be shared is transmitted or disclosed by what methods?
DS personnel are granted access to FAN cloud services to enable them to analyze audit and event information in FAN. This does not require transmission of data.

(e) What safeguards are in place for each internal or external sharing arrangement?
Only personnel authorized with security monitoring responsibilities have access to this information and the ability to generate logs.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
The PII collected is used exclusively to manage access control to the FAN system. The PII is not shared with any other systems or organizations. Access to the PII contained in the system is limited to system administration, support and security personnel with a need to manage access control or monitor the system for security.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals who wish to gain access to or amend records pertaining to them must send an email to CustomerService@state.gov to reach the Bureau of Information Resource Management, Director of Customer Service Office. 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 telephone number where the individual can be reached during normal business hours.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.
Individuals who wish to gain access to or amend records pertaining to them should send an email to CustomerService@state.gov to reach the Bureau of Information Resource Management, Director of Customer Service Office. 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 telephone number where the individual can be reached during normal business hours.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals 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 form which all users must sign to obtain access to the FAN system.

8. Security Controls

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

- User account request form data is stored and protected in the Department myData system and 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 (BoringCrypto).

(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.

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.

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

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

(d) Explain the privacy training provided to authorized users of the system.
Department personnel are required to take the mandatory PII Training, PA459 Protecting Personally Identifiable Information, and DOS Cyber Security Awareness Training.

(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.

FAN Google G Suite system implements FIPS PUB 140-2 approved encryption modules for data at rest, data transmission and backups. The configuration of the FAN Google G Suite service is centrally administered by IRM/FO authorized system administrators.

Access and authentication to FAN is controlled through the Google-provided identity and access management system which is configured to use multi-factor authentication with strong passwords.

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

FAN implements, at a minimum, security controls required for cloud computing moderate impact systems. In addition, FAN implements Privacy Controls specified in NIST SP 800-53 Rev 4 as well as additional security controls from NIST SP 800-53 Rev 4 selected for processing of Consular, Financial, Medical, and Personnel (HR) data. Together, these controls ensure that security and privacy controls are in place to protect the types of PII and other State Department Sensitive But Unclassified (SBU) information processed in FAN.

9. Data Access

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

Users only have access to their information and other information which they are granted access based on their organization, role and determination of the information owner.

With regard to PII used to support user account request processing, FAN Enterprise Support Personnel have access to this data as necessary to perform their assigned role.

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

FAN leverages OpenNet account and access authorization processes which include an access request form. FAN augments this existing process with FAN-specific processes to ascertain initial user account and access. Existing OpenNet policy regarding delegation of access control to bureaus, embassies and posts is implemented by FAN to empower personnel at the office level to implement access control to data. The FAN information system security officer (ISSO) monitors FAN configuration and access grants for policy violations and initiates tickets to address issues when detected.

(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.

User access to information in the system is restricted based on their organization, role, and need to know. User access to account PII is restricted to personnel with a need to manage or monitor access to the system.

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

All access to the system, its services, functions, and information is audited. This audit data is collected and analyzed by FAN security officers and DS personnel to detect inappropriate use.