Submit the completed PIA to
Privacy's SharePoint Customer Center

PEPFAR Regional Planning Meetings on FAN

1. Contact Information

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

2. Information on the Collection

(a) Name of collection: PEPFAR Events and Meetings

(b) Bureau: S/GAC

(c) Collection acronym: PEPFAREM

(d) iMatrix Asset ID Number: 212914 (FAN iMatrix ID)

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

☒ New collection

☐ Significant modification to an existing collection

☐ Triennial update for this collection

(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Describe the purpose of the collection:
The purpose of this collection is to determine who will be attending PEPFAR meetings/conferences and to sort the attendees into different groups based on their technical expertise and program country affiliation. We will have space constraints at our venues and we use the FAN as a registration feature to ensure we work within those constraints.

(b) Describe the personally identifiable information (PII) that is collected, used, maintained, or disseminated:
The PII in this collection is from both U.S persons and non-U.S persons and includes first name, last name, email address, phone number, address, passport info, emergency contact information.

(c) What are the specific legal authorities and/or agreements that allow the information to be collected?
The authorities of the Coordinator are under section 201 of The Leadership Against HIV/AIDS, Tuberculosis, and Malaria Act of 2003 (22 USC 265a(f)). Additionally, under the Department of State Foreign Operations, and Related Programs Appropriations Act, 2018 (Div. K, P.L. 115-141).

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

☒Yes, provide:

- SORN Name and Number: Protocol Records, State-33; Volume 81, Number 38
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): February 26, 2016

☐No, explain how the information is retrieved without a personal identifier.
Click here to enter text.

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

If yes, please notify the Privacy Division at Privacy@state.gov.

(f) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this collection? ☒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)): N1-059-09-43, Item 1
- Length of time the information is retained in the collection: Permanent
- Type of information retained in the collection:
  Files contain documents, policy papers, strategic plans, discussion files, briefing books and reports, Summary Reports to Secretary of State, trip reports, agreements, cables, emails, memoranda, and intelligence reference books. The files also include those of the Staff Director and staff members domestically and from posts overseas.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the collection? 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 collection contains Social Security Numbers (SSNs), is the collection necessary?

☐Yes ☐No ☒ Does not contain SSNs

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

(c) How is the information collected?
The information is collected via a Google survey sent to potential attendees/participants from a FAN.gov email address.

(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?

The responsibility is on the respondent to ensure the information provided in their survey response is accurate.

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

The information provided is assumed current as of the date the survey is submitted. No steps are taken to ensure that the information is current unless a discrepancy is discovered (eg. Misspelled name). It is the responsibility of the respondent to update the survey administrators if a change needs to be made.

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

No.

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

The Google survey will have a Privacy Act statement posted on the front page of the survey. Respondents will be notified that their information is being collected in order to register them for a PEPFAREM meeting or event.

(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?

Individuals grant consent by completing the Google Survey sent to them. Their information would not be collected unless they respond /submit the survey. Subsequently, if they do not respond they cannot attend the meeting.

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

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

We seek to collect as little PII as possible while maintaining the ability to monitor who will be attending our meeting.

5. Use of information

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

To monitor and track the participants of a meeting/conference.

(b) Is the use of the information relevant to the purpose for which the collection was designed or for which it is being designed?
Yes, the information would be used solely for PEPFAR meetings/conferences and would not be used or shared for any other purposes.

(c) Does the collection 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?

(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.
Once the PII is collected it is shared externally with the relevant stakeholders for that specific event, which includes U.S. Government Agencies, host governments, non-governmental organizations, multilateral organizations, civil society organizations and implementing partners.

(b) What information will be shared?
The full information will only be shared with the S/GAC logistics team. Externally, only names, titles, emails and organizational affiliation are shared with relevant external stakeholders as a master contact list for the event.

(c) What is the purpose for sharing the information?
Externally, the information is shared as a master contact list with all meeting stakeholders for a specific event to ensure that we can fully execute PEPFAR meetings and events with minimal disruption.

(d) The information to be shared is transmitted or disclosed by what methods?
Only the necessary information is e-mailed to relevant external stakeholders. Each email will contain clear language stating that the information each stakeholder has received is not to be shared with anyone beyond the recipient.

(e) What safeguards are in place for each internal or external sharing arrangement?
The minimum information necessary will be shared externally to safeguard PII. Information shared externally will contain instructions stating that the information contained in the email is not to be shared beyond the recipient.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

A privacy concern would be sharing PII unnecessarily. We only share the minimum amount of PII necessary to collaborate with external stakeholders as needed.

7. Redress and Notification

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

Once they have submitted their information into the survey they would not have access to it. There is no procedure for respondents to access their information.

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

☒Yes ☐No

If yes, explain the procedures.

It is the responsibility of the respondent to alert the survey administrators via email that inaccurate or erroneous information was submitted.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?

Respondents will receive an e-mail with instructions as to how to correct their information.

8. Security Controls

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

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) with FIPS 140-2 approved encryption module (BoringCrypto) protects all data stored in Google G Suite.

(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.

Only members of the S/GAC logistics team have access to the data in the Google team drive. Access will not be granted to anyone who is not a member of the S/GAC logistics team.

(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 authenticate users for access.

(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 R4 as well as additional security controls from NIST SP 800-53 R4 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 collection?
Only those on the S/GAC logistics team.

(b) How is access to data in the collection determined?
Based on the need to perform essential duties as a part of the S/GAC logistics team.

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

(d) Will all users have access to all data in the collection, or will user access be restricted? Please explain.
Only the members of the S/GAC logistics team will have access to all the data in the collection.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
1 – Controls in place for the collection: All access to the sharing functions on Google Sheets and access to the sheets will be limited to the S/GAC logistics team. The S/GAC logistics team is aware that they are not allowed to share access to the master spreadsheet. S/GAC logistics team will ensure compliance with all data storage protocols.

2 – Controls in place for the system: All access to the FAN platform, 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.