Submit the completed PIA to
Privacy's SharePoint Customer Center

INR/AO Collection 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: INR/AO Collection on FAN

(b) Bureau: Intelligence and Research (INR/AO)

(c) Collection acronym: INR/AO FAN

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

(e) Reason for performing PIA: INR/AO process PII on FAN

- ☒ New collection
- ☐ Significant modification to an existing collection
- ☐ Triennial update for this collection

(f) Explanation of modification (if applicable):

3. General Information

(a) Describe the purpose of the collection:
This system allows INR/AO to collaborate with contractors (using a Department-managed cloud computing solution) to identify and assess potential participants in INR-sponsored analytic exchanges. INR/AO, per 1 FAM 423.4, "Organizes and funds analytic exchanges with outside experts to inform the thinking of U.S. Government policymakers and intelligence analysts." This collaboration will allow INR/AO to carry out its mission more efficiently and effectively.

(b) Describe the personally identifiable information (PII) that is collected, used, maintained, or disseminated:
The PII in this collection is derived from open-source (Google/public web) searches for publicly available information on potential participants in analytic exchanges. This information could include name, date of birth (or estimated DOB), home and work address, work organization, country of citizenship, gender, birthplace, and driver's license or passport number. All information input into this collection will be from publicly available sources only.

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

INR is authorized to "collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions" under section 1.7(i) of Executive Order 12333.

(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)
- 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.

(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 Office 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)): GRS 17, Item 006: A-17-006-01a / N1-059-91-18, item 23a
- Length of time the information is retained in the collection: Indefinitely.
- Type of information retained in the collection: Contract research files

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?

(c) How is the information collected?
INR/AO and its contractor may collect information/PII of potential INR/AO event participants from public web searches.

(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?

INR/AO and/or its contractor ensure that any PII collected is from a reliable public source (for example, collecting the work address and organization name from the website of the organization itself, or from a CV posted directly by the individual). Once an individual has agreed to participate in or support an analytical exchange, INR/AO and/or the contractor will contact the individual directly to confirm the accuracy of information.

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

INR/AO and/or its contractor checks reliable public sources (i.e. the website of an individual's employer) to keep information current, and may also directly confirm the accuracy of information with the individual. Information may be retained (and updated at a later date) in case INR/AO considers an individual for participation in or support of a future analytical exchange.

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

Yes, INR/AO and the contractor use publicly available information (obtained from the internet, newsfeeds, or from state or local public records, etc.). INR/AO and the contractor do not plan to collect information from subscription-based commercial databases.

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

INR/AO does not provide notice to an individual, whom it is considering as a potential participant in an analytical exchange, since it collects the information from publicly available sources (the Internet, news feeds, organizational websites, etc.) and not from the individual directly.

(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?

Per 3(b), INR/AO and its contractor collect only publicly available information on potential speakers. It is not reasonable for INR/AO and its contractor to notify each potential speaker about this collection while still in the process of determining a potential speaker's suitability for an analytical exchange.

(j) How did privacy concerns influence the determination of what information would be collected?
INR/AO and its contractor collect only the minimum amount of PII needed to conduct government business and administer analytic exchanges. To ensure protection of PII, INR/AO will own all documents that are part of this collection and control all permissions for documents, in order to ensure that only those with a strict need-to-know outside of INR/AO have access to this information.

5. Use of information

(a) What is/are the intended use(s) for the information?
The information will be used to identify and assess potential participants in INR/AO events, to ensure that their participation in an exchange will not negatively impact the U.S. government or State Department.

(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. INR/AO has selected a secure system, FAN, to increase the efficiency of collaboration with its contractor. The use of this platform is in line with the Secretary of State's initiatives on increasing use of cloud-based technology.

(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?
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.
No routine internal sharing occurs outside of INR/AO. On a case-by-case basis, INR/AO expects to grant external ad-hoc access to documents to employees of an INR contractor working outside of OpenNet (to input information collected by the contractor from publicly available sources).

(b) What information will be shared?
All information that is part of the collection will be shared.

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

The purpose of sharing the information is to allow INR/AO to use the services of a contractor to more efficiently identify and assess potential participants in INR/AO analytic exchanges. INR/AO and its contractor collaborate on inputting this information. Many of INR/AO's exchanges are implemented through the contractor.

(d) The information to be shared is transmitted or disclosed by what methods?
The information will be shared within the FAN system via 1) Google Drive Folder shared with users, and/or 2) specific Google Docs, Sheets, Slides, or Forms shared with users on a strict need-to-know basis.

(e) What safeguards are in place for each internal or external sharing arrangement?
INR/AO will maintain control over permissions for all documents that are part of the collection, to ensure that only employees and contractors with a need-to-know" have access to the information. Once the contractors no longer need access to the document, INR/AO will remove their access permissions. In addition, the agreement between INR and the contract will specify the contractor's responsibility to take special precautions to protect any PII collected or accessed.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
INR/AO has worked with the IRM/FO FAN System Owner to identify a solution that specifically safeguards privacy. Previously, INR/AO and its contractor collected and shared PII to facilitate the payment of fees and/or honoraria via email. Sharing and collaborating on the collection of this information via FAN improves business efficiency and the accuracy of information collected, is a more secure method of sharing information than email, and reduces the risk that PII will be compromised.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Individuals should follow the instructions for gaining access to their information as stated in the covering SORN, State-33 Protocol Records.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.
Individuals should follow the instructions for gaining access to, and correcting, their information as stated in the covering SORN, State-33 Protocol Records. An individual must specify that he or she wishes the records of the INR/AO Collection on FAN to be checked.

If no, explain why not.
Click here to enter text.

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

INR/AO does not notify potential speakers of procedures to correct their information. Per 4(h), INR/AO does not inform potential speakers that INR/AO and/or its contractor are collecting publicly available information on them.

8. Security Controls

(a) How is the information in the collection 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) that 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.

INR/AO will use the following procedures to limit access: 1) Use FAN Google sharing feature to ensure only authorized persons are invited and approved for access to PII; 2) Use FAN Google sharing feature for access control to implement least privilege access to the PII and restrict level of access (view, comment, edit) and where appropriate limit download and printing; and 3) Use FAN Google access control feature to require all personnel to authenticate to FAN prior to access.

(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.

Separately, INR/AO will follow the following procedures: 1) Review user access to PII at least every 90 days to identify persons to be removed from access; 2) Review user access level to PII every 90 days to identify changes to ensure least privilege; 3) Retain a record of conduct of these reviews; and 4) Remove all PII from the collection when the need no longer exists, and notify FAN Support.

(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 which has a privacy component.

(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 to 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?

INR/AO employees with a need-to-know can create and manage permissions for documents in the system. INR/AO employees may grant permission to specific contractors to access individual documents if they have a "need to know" for specific PII.

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

INR/AO will only give access to employees who have a strict business need-to-know and who are directly involved in the administration of the analytic exchange program. Separately, INR/AO will only give access to contractor employees who are directly involved in the planning of an analytic exchange and have been previously identified by the contractor as employees for this task. This access will be given on an individual user (i.e. not group or anonymous) basis to ensure access to the data is as restricted as possible.

(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.

INR/AO will arrange for FAN accounts to be provided to employees with a business need-to-know. Employees with FAN accounts will have access to all data in the collection. INR/AO will provide user access to any non-INR/AO individuals on a case-by-case basis based on a direct need to know. INR/AO employees with FAN accounts will manage granting of such permissions.

(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: INR/AO management will instruct its employees to regularly monitor the quality and accuracy of information collected by the contractor. In addition, INR/AO management will conduct periodic spot checks of the Google documents in which the information is stored, to include spot checks of the permissions granted for each document, to ensure only users with a strict need-to-know have access to the information. After the conclusion of an analytic exchange, INR/AO will remove the contractor's permissions to access documents relating to that specific exchange.

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. INR/AO will only request FAN accounts for its employees who have a need to use this system.