PRIVACY IMPACT ASSESSMENT

FREEDOMS2

1. Contact Information

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

2. System Information

a. Date of completion of this PIA: July 2022
b. Name of system: FREEDOMS2
c. System acronym: N/A
d. Bureau: Administration
e. iMatrix Asset ID Number: 514
f. Child systems (if applicable) and iMatrix Asset ID Number: None
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:

The FREEDOMS2 system is the primary case processing system for the Department's information access program. FREEDOMS2 receives copies of records, in both soft and hardcopy formats, ingests them for electronic review, redaction, and release commensurate with established program procedures and under the purview of the various information access mandates (e.g., the Freedom of Information Act, the Privacy Act, Mandatory Declassification Review under E.O. 13526, etc.) answered to by the Office of Information and Program Services (IPS). As the primary case processing system for the Department's centralized information access programs, FREEDOMS2 ingests a wide variety of records created and maintained by the Department. As such, any PII captured

from these documents would be presented to FREEDOMS2 users for review, redaction, and release.

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

At a minimum, FREEDOMS2 collects from requesters:

- Full Name
- Address
- Email Address
- Phone Number

In the case of Privacy Act requests, where requesters are either U.S. citizens or legal permanent residents (LPRs), individuals* are also required to submit:

- Place of Birth
- Date of Birth
- Citizenship Status

* "[T]he term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(a)(2).

Finally, in the case of requests for Visa records, the requester submits:

- Place of Birth
- Date of Birth
- Citizenship Status

Although Freedoms2 does not request or require SSN and Alien Registration numbers, information requesters sometimes volunteer this information to help track their request in the system.

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

5 U.S.C. § 552 – Public information; agency rules, opinions, orders, records, and proceedings
5 U.S.C. § 552a(d) – Records maintained on individuals: Access to Records
22 C.F.R. §§ 171.10-171.18 – Public Access to Information: Freedom of Information Act Provisions
22 C.F.R. §§ 171.20-171.26 – Public Access to Information: Privacy Act Provisions
22 CFR § 171.22(c) - Verification of Personal Identity

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

☒Yes, provide:

- SORN Name and Number: Information Access Programs Records, State-35
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): August 13, 2012

☐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-06-015-03b(1), A-06-015-03b(2), A-06-015-03d, A-06-015-03e, A-06-015-03e, A-06-015-03f, A-06-015-03g, A-06-015-03h, A-06-015-03i, A-06-015-03j, A-06-015-03k, A-06-015-04, A-06-015-05, A-06-015-06 and A-06-015-07

- Disposition Authority Number: N1-059-10-16, item 1b(1), N1-059-10-16, item 1b(2), N1-059-10-16, item 1d, N1-059-10-16, item 1e, N1-059-10-16, item 1f, N1-059-10-16, item 1g, N1-059-10-16, item 1h, N1-059-10-16, item 1i, N1-059-10-16, item 1j, N1-059-10-16, item 1k, GRS 5.2, item 020, N1-059-10-16, item 3, GRS 3.1, item 051 and GRS 3.2, item 051

- Length of time the information is retained in the system: Up to 30 years

- Type of information retained in the system:
  As per the FREEDOMS2 Disposition Schedule, the system retains master electronic case file information (information specific to the processing of the case, to include requester information), digitized source documents (records responsive to information access requests), case management and statistical reports, system documentation, and system backups.

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
☒ 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
Although FREEDOMS2 does not request SSN and Alien Registration numbers, information requesters sometimes volunteer this information to help track their request in the system.

– If yes, under what authorization?

d. How is the PII collected?

Information access programs - case specific information is supplied by the requester, as part of their request for information. When they file their request (via letter, facsimile, or online submission at https://foia.state.gov/Request/Submit.aspx), this information is supplied along with other parameters provided to identify, locate, and retrieve the records to which they seek access.

Documents obtained as result of an information access request – any PII residing within the body of records contained within FREEDOMS2 – would have been collected by the original collecting office/bureau/post prior to retrieval and submission to IPS in conjunction with an information access request. Those records are then ingested into FREEDOMS2 for review, redaction, and release.

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.

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

The information contained within the information access request is provided by the requester themselves. The PII in question is their own information, the accuracy of which is necessary to access government records.

The initial collecting office/bureau/post that is processing the request is responsible for the accuracy of the information contained within any records retrieved.

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

Yes, PII provided by the requester is used to either correspond with said requester, or to identify, locate, and retrieve the records sought by the requester.

Currency of the information in the Department's record keeping system is the responsibility of the records custodians (e.g., the bureau, post, office) who search for and respond to a search tasking.

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

FREEDOMS2 does not use information from commercial sources. IPS case managers can use publicly available sources of information to locate a requester.

i. How was the minimization of PII in the system considered?
IPS limits the amount of PII required to initiate and process most cases to full name, address, email address if available, and phone number. For Privacy Act requests, the Department requires additional information limited to date and place of birth and citizenship status.

5. Use of information

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

The intended use of the information (e.g., name and address) is to correspond with and mail released records to the requester.

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, the use of the information is pertinent to the processing of information access requests.

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: The requester information is potentially shared with the following custodial record keepers in the event of a request for personal information: Bureau of Diplomatic Security, Bureau of Medical Services, Bureau of Consular Affairs, and the Bureau of Human Resources.

External: The requester information is potentially shared with other government agencies (such as the Department of Homeland Security) in conjunction with privacy referrals/consultations.

b. What information will be shared?

Internal: The requester-provided information (e.g., name, address, etc.) will be used to create the electronic case file. The original request itself (which may contain this information) may be shared with the custodial record keepers for the purposes of locating the records sought by the requester.

Any PII that is contained within the records sought by the requester, supplied by the original collecting office/bureau/post to IPS for the purposes of records review/redaction, will be shared with those employees who have a need-to-know so they can process the information requested.

External: Where coordination with other government agencies is necessary, the requester-provided information is shared. In those instances where documents that were created by another agency are in possession of the Department of State, the Department could potentially provide to that agency their record for their release determination.

c. What is the purpose for sharing the information?

Internal: The purpose for sharing information provided by the requester (e.g., name and address) is to process the requested information, and draft correspondence to the requester.

In the event of PA cases, the requester-provided information (e.g., DOB/POB/citizenship) is used to validate the request under the access provision requirements set forth in 5 U.S. Code § 552a, and for the purposes of locating the responsive records sought by the requester (e.g., passport records, visa records, etc.).

External: The purpose for sharing information with other government agencies is to facilitate the retrieval of relevant information by that agency. In cases where records retrieved by the Department of State are, in fact, another agencies' record, the information is shared for the purposes of processing the request (i.e., to ensure that the requested information is released only to the person who is requesting the information and that that person has a right to the requested information).

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

Internal: The requester-provided information that is used to create the electronic case record and to administer the processing of the case is sent through the interoffice mail system or the OpenNet/ClassNet email systems.

External: Documents sent to other government agencies are hand-carried by authorized personnel or sent via secure facsimile.

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

Internal: Department users with FREEDOMS2 accounts send approved information to authorized offices and the case officer who will respond to the request and send external correspondence. The correspondence is either through the Department's OpenNet/ClassNet email systems or hand-carried by authorized personnel (a signature is required by receiving office).

External: External correspondence is sent by authorized personnel in a secure envelope. A signature is required upon receipt of the information.

7. Redress and Notification

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

Notice for the direct collection of an individual's information, in conjunction with the initiation of an information access case, is provided through our procedures published in 22 CFR 171, the Department's FOIA website, and System of Records Notice State-35. No information is collected without the written and signed request and authorization by the record subject.

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 an individual declines to provide the requisite PII during the case initiation phase (e.g., name and address at a minimum), then their case is simply closed in 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?

A case manager will assist a requester with gaining access to their information. A requester can also follow the procedures outlined in SORN State-35 to gain access to their information. For Privacy Act requests, it may be necessary to accompany a request to gain access to this information with a written, singed statement indicating that they are the individual requesting access to the information.

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

☒Yes ☐No

If yes, explain the procedures.

A requester contacts the FOIA hotline (by phone, mail, or email) and a case manager will assist with their information access request, or they can file a Privacy Act request to amend to records that are not accurate, relevant, timely or complete.

In the case that an individual wishes to have records located within FREEDOMS2 corrected they need to contact the owning office/bureau/post, which originally collected the information, to have it amended. This process is described in SORN State-35.

If no, explain why not.

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

Record subjects are notified of the procedures to correct their information through an initial response letter, the Department's FOIA website, 22 CFR 171 and SORN State-35.

8. Security Controls

a. How is all of the information in the system secured?

FREEDOMS2 resides on the Department's ClassNet general support system. FREEDOMS2 utilizes single sign-on authenticated with a user's ClassNet account and an established FREEDOMS2 account. FREEDOMS2 is physically limited to the Harry S Truman Building, the headquarters of the United States Department of State. To gain

access to the information within FREEDOMS2, a user needs to hold a security clearance of SECRET or higher, be on the approved access list to the Harry S Truman Building, possess a ClassNet account, possess a FREEDOMS2 application account, and possess a FREEDOMS2 database account. Access to FREEDOMS2 is physically limited to a Diplomatic Security-certified secure work area (SWA). Furthermore, to have access for any PII beyond the minimum requirement of requester name and address (e.g. full-name, place and date of birth, citizenship status, etc.), the user must be designated as an employee of a case processing group with an approved need for access.

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).

FREEDOMS2 has roles for Systems Administrators, Super Users (Branch Chiefs and Team Leaders), and Users. The System Administrator role has permissions to control all objects in FREEDOMS2. The Super User role has elevated permissions to allow the Super User to move work items around in the workflow. The User role has minimal permissions, limited to those required to complete routine assigned tasks. The System Administrators, Super Users, and Users all have access to the personally identifiable information (PII) that the system collects, uses, maintains, and disseminates.

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 is limited to those having an official need to access the information in their work capacity by the establishment of case processing groups. The case processing group only has access to the records assigned to that specific group. They cannot access any other records outside of those assigned to their group.

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

Only approved systems administrators are appointed by the system owner. Super users are appointed by their supervisors with system administrator and system owner approval. Users are appointed by their supervisor and the system administrator, or a designated representative will create the account to give the user access to the data in the system.

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

FREEDOMS2 has full auditing capabilities attributed down to the user account. This functions in conjunction with the safeguards provided by the general support system, ClassNet. Each case in FREEDOMS2 can be marked a "Privacy Case". If a case is marked "Privacy", the case cannot be searched, viewed or accessed unless a user is a member of the Privacy Access Control List. This allows for only a very small number of users to access Privacy cases. Active monitoring is conducted by ClassNet as the general support system. Access to privacy case information is limited by the system controls.

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.

Case analysts are provided training on the Privacy Act and its provisions, both by the U.S. Department of Justice training series, as well as internally by IPS. Users are required to take the mandatory FSI course PA 318 Protecting Personally Identifiable Information biennially and PS800 Cybersecurity Awareness annually.