Office of Information Policy

Privacy Impact Assessment
for the
FOIA System for Tracking Requests and Appeals (FOIA STAR)

Issued by:
Senior Component Official for Privacy,
Lindsay Steel, Chief, Compliance Staff

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: August 11, 2021

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

FOIA System for Tracking Requests and Appeals (FOIA STAR) is a web-based application utilized by the United States Department of Justice (DOJ or "the Department"), Office of Information Policy (OIP), to oversee the Department's obligations under the Freedom of Information Act (FOIA), among other federal disclosure laws. The system facilitates the submission, tracking, and case management of FOIA and Privacy Act (PA) initial requests, and the administrative appeals of denied access to records requests issued by Department components under the FOIA and PA. FOIA STAR also allows for the case tracking of Mandatory Declassification Review Requests (MDR), inquiries submitted to OIP regarding federal agency compliance with the FOIA, and FOIA litigation. FOIA STAR serves as an electronic records management system. FOIA STAR stores FOIA and PA requests and appeals, notes and correspondence related to requests and appeals, appeal background information, and OIP's responses to requests and appeals, along with information pertaining to MDRs, compliance inquires, and FOIA litigation. FOIA STAR will also be used to facilitate the Department's preparation of Annual FOIA Reports.

The system is used to collect, maintain or disseminate the following types of personal information: requester name, alias, home address, telephone number, email address, file/case ID numbers, and work-related information for business representatives or attorneys representing requesters. While the Department does not require individuals to provide their Social Security Numbers (SSNs), some requesters may voluntarily provide their SSNs in their requests or certifications of identity, which FOIA STAR would then maintain.

Information in FOIA STAR may be used by and shared between OIP staff members, other Department components, and other Federal entities to efficiently and effectively respond to FOIA requests and appeals. Some system information, which may include personally identifiable information (PII), is shared with Tyler Technologies, Inc. for the limited purposes of hosting, maintaining, and resolving issues related to FOIA STAR. OIP is responsible for day-to-day user administration.

OIP conducted this Privacy Impact Assessment (PIA) because FOIA STAR maintains and collects information about FOIA and PA requesters who submit requests and appeals to OIP. Although it may be possible for other Department components to utilize the application and tailor the platform to their own needs, this PIA is limited to OIP's use of FOIA STAR.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

OIP oversees the Department's obligations under the FOIA. OIP adjudicates administrative appeals of denied access to records requests processed by Department components under the FOIA and the PA; processes FOIA and PA initial requests for records of the Offices of the Attorney General, Deputy Attorney General, Associate Attorney General, and other Senior

Management Offices; provides staff support for the Department Review Committee, which reviews Department records containing classified information; responds to inquiries submitted to OIP regarding federal agency compliance with the FOIA; responds to Executive Secretariat matters; and provides counsel for and handles the defense of certain FOIA matters in litigation. OIP is also responsible for preparing the Department's Annual FOIA Reports. FOIA STAR will allow Department components to submit their Annual FOIA Report data to OIP for review and compilation into the Department's final report. FOIA STAR will assist OIP in executing these responsibilities effectively and efficiently.

Requesters may submit requests or appeals electronically to FOIA STAR using their FOIA STAR user account. Instructions for accessing FOIA STAR and creating a user account are available at https://www.justice.gov/oip/submit-and-track-request-or-appeal. Requesters may also submit requests electronically through the National FOIA Portal on FOIA.gov, which will transmit the request directly into FOIA STAR via an Application Programming Interface (API). If needed, the requester may certify their identity electronically by uploading necessary documentation, such as a completed DOJ-361 Form, as part of their request submission, whether submitted through FOIA STAR or FOIA.gov. Requesters may also submit requests and appeals by postal mail. OIP staff manually input a requester's information into FOIA STAR if the request or appeal is received by postal mail. Once a request or appeal is in the system, OIP staff will begin processing it in FOIA STAR. Responses to requests and appeals are generally transmitted electronically to the requester via email, which may be sent either automatically from FOIA STAR or manually outside of the system. Responses may be transmitted via postal mail if preferred by the requester.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

	Authority	Citation/Reference
	Statute	5 U.S.C. § 552, the Freedom of Information Act 5 U.S.C. § 552a, the Privacy Act 44 U.S.C. § 2201, the Presidential Records Act
	Executive Order	Exec. Order No. 13,526 (Dec. 29, 2009)
	Federal Regulation	28 C.F.R. Part 16; 28 C.F.R. Part 17
	Agreement, memorandum of understanding, or other documented arrangement	N/A
	Other (summarize and provide copy of relevant portion)	N/A

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of

information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	Names of OIP and DOJ component employees/contractors; other gov't personnel who may be contacted in processing requests or handling FOIA appeals/litigation; names of FOIA/PA requesters (USPER and non-USPER)
Date of birth or age	X	C, D	This information may be contained in a FOIA/PA request, requester's certification of identity, and/or in records responsive to a FOIA/PA request
Place of birth	X	C, D	This information may be contained in a FOIA/PA request, requester's certification of identity, and/or in records responsive to a FOIA/PA request
Gender	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Race, ethnicity or citizenship	X	C, D	This information may be contained in a FOIA/PA request, requester's certification of identity, and/or in records responsive to a FOIA/PA request

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Religion	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Social Security Number (full, last 4 digits or otherwise truncated)	X	C, D	This information may be contained in a FOIA/PA request, requester's certification of identity, and/or in records responsive to a FOIA/PA request
Tax Identification Number (TIN)	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Driver's license	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Alien registration number	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Passport number	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Mother's maiden name	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Vehicle identifiers	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Personal mailing address	X	C, D	Personal contact info for requesters
Personal e-mail address	X	C, D	Personal contact info for requesters
Personal phone number	X	C, D	Personal contact info for requesters
Medical records number	X	C, D	This information may be contained in records responsive to a FOIA/PA request

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Medical notes or other medical or health information	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Financial account information	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Applicant information	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Education records	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Military status or other information	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Employment status, history, or similar information	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Certificates	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Legal documents	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Device identifiers, e.g., mobile devices	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Web uniform resource locator(s)	X	C, D	This information may be contained in records responsive to a FOIA/PA request

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Foreign activities	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Juvenile criminal records information	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Civil law enforcement information, e.g., allegations of civil law violations	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Whistleblower, e.g., tip, complaint or referral	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Grand jury information	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Procurement/contracting records	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Proprietary or business information	X	A, B, C, D	This information may include business contact info for gov't employees and some requesters; this info may be contained in records responsive to a FOIA/PA request
Location information, including continuous or intermittent location tracking capabilities	X	C, D	This information may be contained in records responsive to a FOIA/PA request
Biometric data:			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Photographs or photographic identifiers**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **Video containing biometric data**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **Fingerprints**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **Palm prints**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **Iris image**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **Dental profile**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **Voice recording/signatures**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **Scars, marks, tattoos**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **Vascular scan, e.g., palm or finger vein biometric data**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **DNA profiles**	X	C, D	This information may be contained in records responsive to a FOIA/PA request
- **Other (specify)**			
System admin/audit data:			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **User ID**	X	A, C, D	User information will be collected for agency users and requesters who create a user account
- **User passwords/codes**	X	A, C, D	User information will be collected for agency users and requesters who create a user account
- **IP address**	X	A, C, D	User information will be collected for agency users and requesters who create a user account
- **Date/time of access**	X	A, C, D	User information will be collected for agency users and requesters who create a user account
- **Queries run**	X	A, C, D	User information will be collected for agency users and requesters who create a user account
- **Content of files accessed/reviewed**	X	A, C, D	User information will be collected for agency users and requesters who create a user account
- **Contents of files**	X	A, C, D	User information will be collected for agency users and requesters who create a user account

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible): FOIA STAR will retain all final responses, which includes any responsive records that OIP processes and releases to a requester. In narrow circumstances, the final response disclosed to the requester may include PII approved for disclosure in accordance with Federal law and DOJ policy. Because of the varied nature of the records that may be subject to disclosure and because the responsive records maintained in FOIA STAR could conceivably include almost any type of information, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by FOIA STAR.	X	A, B, C, D	This information may be contained in records responsive to a FOIA/PA request

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify): If an individual is represented by an attorney, the attorney may provide information on the client's behalf. Because the attorney acts as the client's representative, OIP considers any personal information provided by an attorney as submitted by the individual client.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other Federal Entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		

Government sources:
Other (specify): Other federal entities that are consulting with or referring FOIA-requested records to OIP for processing. State, local, tribal, and foreign entities may be FOIA requesters submitting requests or administrative appeals through the methods already outlined in Section 2.1. Additionally, records that are responsive to FOIA requests or communications concerning FOIA requests, which are also stored in the system, may consist of information provided by the above sources.

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
Other (specify): Any of the above categories may be FOIA requesters submitting requests or administrative appeals that will be stored in FOIA STAR. Additionally, records that are responsive to FOIA requests or communications concerning FOIA requests, which are also stored in the system, may consist of information provided by the above sources.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	Internal DOJ/OIP employees and contractors have direct access to the system.
DOJ Components	X		X	DOJ component users will have direct log-in access for the sole purpose of submitting Annual FOIA Report data to OIP and receiving data validation results. Other information contained in FOIA STAR but accessible only by OIP staff may be shared with DOJ components in order to process FOIA requests and appeals.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal entities	X			Information may be shared with other Federal entities in order to process FOIA requests and appeals.
State, local, tribal gov't entities	X			Information may be shared with other State, local, tribal gov't entities in order to process FOIA requests and appeals.
Public	X			Information may be shared with requesters in order to process FOIA requests and appeals they have submitted. Information will also be shared with the public as required to fulfill the Department's reporting and proactive disclosure obligations under the FOIA. Methods of sharing responsive information are detailed in Section 2.1.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Information may be shared if a FOIA request or appeal becomes the subject of litigation.
Private sector			X	Information will be shared with Tyler Technologies, Inc., for the limited purpose of hosting and administering FOIA STAR.
Foreign governments	X			If a foreign government has submitted a FOIA request or appeal, OIP's final response and any responsive documents will be shared with this requester.
Foreign entities	X			If a foreign entity has submitted a FOIA request or appeal, OIP's final response and any responsive documents will be shared with this requester.
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

Information contained in the system will be released to the public in two ways: 1) through the monthly postings of OIP's FOIA Logs available in OIP's FOIA Library, and 2) as part of the Department's Annual FOIA Report in aggregate and raw data formats.

The FOIA Logs include the request subject, tracking number, submitted date, closure date, and disposition details for requests processed by OIP. The logs do not identify the requester and do not include any first party requests submitted by or on behalf of individuals asking for their own records.

The Annual FOIA Report[1] includes data pertaining to any requests, consultations, and administrative appeals that OIP received, processed, or had pending during a given fiscal year. The Annual FOIA Report contains various aggregate statistics. The accompanying raw data contains information about the processing of each request as identified by tracking number and does not contain any information about the identity of the requester or subject of the request.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Notice is provided to individuals informing them about the collection, use, sharing or other processing of their PII pursuant to a system of records notice published in the Federal Register, JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records. The FOIA STAR system also includes a privacy and security notice that informs requesters of the information collection, as well as a link to the DOJ Privacy Policy, on the login screen.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

FOIA STAR is an optional system through which individuals may submit FOIA or PA requests. Individuals may also use the National FOIA Portal on FOIA.gov to submit requests, which will be transmitted automatically via API to FOIA STAR for processing. Individuals may also submit FOIA and PA requests via mail and OIP will manually enter this information into FOIA STAR for tracking purposes.

[1] https://www.justice.gov/oip/reports-1#s1.

An individual is not required to file a FOIA or PA request, but if an individual wishes to file a request and does not provide the requested information, OIP is unable to process the request. A requester may also decline to provide information by not responding to a notice from OIP that the request does not comply with regulations, for example, if a requester is seeking records about himself/herself and does not provide the appropriate certification of identity. OIP is also unable to respond to any requester that does not provide adequate contact information.

If a requester or appellant uses FOIA STAR to communicate with OIP, then the requester or appellant could decline to provide some general personal data or work-related data. However, the requester or appellant would at least need to provide an email address or physical mailing address to receive a response from OIP.

A person seeking records under the PA who does not provide adequate identifying information under 28 C.F.R. § 16.41(d) will only receive information under the FOIA.

By submitting a proper FOIA or PA request, administrative appeal or other request that utilizes FOIA STAR, an individual provides information for OIP to respond to the request or appeal. OIP maintains this information in FOIA STAR, whether the requester uses FOIA STAR or FOIA.gov to submit their request electronically or OIP manually enters the request information into FOIA STAR. If an individual does not provide the requested information, OIP cannot respond. Applicable provisions of the PA and System of Records Notices, however, limit the use of the information.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

The System of Records Notice DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, as well as 28 C.F.R. Part 16, Subpart D, provide procedures for individuals to access and request amendment or correction of records pertaining to them that are maintained in FOIA STAR. As described in DOJ-004 and pursuant to 28 C.F.R. Part 16, Subpart E, some information maintained in FOIA STAR may be exempt from the access and amendment provisions of the Privacy Act. Generally, OIP does not have the authority to make substantive corrections to underlying records responsive to a FOIA or PA request or appeal that may be maintained in FOIA STAR.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** December 18, 2019 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** No applicable POAMs.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** FOIA STAR is also in continuous monitoring in which security and privacy controls are assessed annually to ensure proper implementation.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** FOIA STAR is a customized version of MicroPact Product Suite, a commercial off-the-shelf application which contains a built-in Audit Reporting Module. The MicroPact Product Suite application audit logs are reviewed and made available to the administrator and system owner through the application's audit module.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: All OIP employees and contractors are required to complete annual privacy training. OIP does not have system-specific privacy training.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

OIP has implemented a number of protections to mitigate the risk of unauthorized access. For example, FOIA STAR will employ two-factor authentication and currently employs role-based access controls to ensure data is handled, retained, and disposed of appropriately. The role-based access controls allow the system administrator to grant access to information based on a least

privilege access setting. Users also sign rules of behavior. The system administrator creates and suspends accounts as part of the new account and account closure process. Additionally, all Department users must complete annual Department security awareness training. An OIP Administrator has access to the audit logs that display user access and roles. This can be periodically reviewed to ensure that users are working in their least privileged access role (for those with multiple roles). Generally, OIP users can access all records in the system, but there are limitations on editing certain types of records depending on the user's role. In addition, data is encrypted at rest within the database and while in transit.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Records maintained in FOIA STAR are retained and disposed of in accordance with record retention schedules approved by the National Archives and Records Administration (NARA). NARA's General Records Schedule (GRS) 4.2, Information Access and Protection Records, controls the retention and destruction of records pertaining to information service functions performed by agencies, including the FOIA, Privacy Act, and Mandatory Declassification Review (MDR) files. Presidential Records Act Requests, inquiries submitted to OIP regarding federal agency compliance with the FOIA, and Executive Secretariat matters are included in OIP's information services functions. Under GRS 4.2, agencies may retain FOIA, Privacy Act, and MDR records for a maximum of six years after final agency action, and litigation records for a maximum of three years after final adjudication by the courts, whichever is later, unless a business use authorizes longer record retention. FOIA STAR contains an internal records management feature that categorizes the information based on the appropriate records retention schedule, automatically notifies the records manager if there are records eligible for disposition, and permits the records manager to review and confirm records for disposal.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

____ No. __X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, 77 FR 26580 (5-4-2012) (last published in full); 82 FR 24151, 152 (5-25-2017).

JUSTICE/DOJ-002, DOJ Computer Systems Activity & Access Records, 64 FR 73585 (12-30-1999) (last published in full); 66 FR 8425 (1-31-2001); 82 FR 24147 (5-25-2017).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

The privacy risks to retaining data in the FOIA STAR system include unauthorized access to the system and compromise of the data by an internal user. In order to mitigate these risks, information and records maintained in the system are only collected and stored as a result of a specific request for information. Information collected in the system is provided by requesters and system users. While most fields in the system can be searched using FOIA STAR's standard and advanced search capabilities, information is generally retrieved based on the individual's name, the tracking number OIP assigned to the matter, the subject matter, or date of the request.

Information is shared internally within OIP, Department component FOIA points of contact, and other federal entities only as needed, and on a case-by-case basis to the extent necessary for processing requests and appeals. Information may be shared with individual requesters to assist in processing requests or appeals that they have submitted. Role-based access controls allow the system administrator to grant access to information based on a least privilege access setting. Users also sign Rules of Behavior. The system administrator creates and suspends accounts as part of the new account and account closure process.

Privacy notice is provided to individuals informing them about the collection, use, sharing or other processing of their PII pursuant to a system of records notice published in the Federal Register. The FOIA STAR system also links to the Department's Privacy Policy and includes a security notice that informs requesters of the information collection.

The administrative, technical, and physical controls are addressed within the security control assessment as part of FOIA STAR's continuous monitoring. At the end of each authorization period, the system Authorizing Official review the ATO package and makes an informed risk-based decision on the operational status of the system.