Justice Management Division

Privacy Impact Assessment
for the
National Freedom of Information Act Portal

Issued by:
Morton J. Posner
Senior Component Official for Privacy

Approved by: Jay Sinha
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: March 17, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or information technology, its purpose, how it operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The National Freedom of Information Act Portal (NFP), also referred to as FOIA.gov, is a public-facing website allowing the public to submit requests for government records to any federal agency from a single interface ("portal"), pursuant to the Freedom of Information Act (FOIA) Improvement Act of 2016.[1] The information submitted in a FOIA request, or a Privacy Act of 1974 ("Privacy Act") access request, where applicable[2], via the public-facing website (https://www.foia.gov) is automatically delivered to the requester-designated federal agency for ingestion into the agency's FOIA request tracking system; agencies retain authority to create and maintain their independent request tracking systems.

The Justice Management Division (JMD) conducted a Privacy Impact Assessment (PIA) for NFP, published in 2022, because this system maintains and collects information about requesters and certain federal agency personnel. A requester is not required to create an account in order to submit a request. However, personal contact information is necessary for the designated federal agency to correspond with the requester. NFP user accounts exist for Agency Managers so that requests can be delivered within the system and processed outside of the NFP in accordance with the FOIA statute by each agency's FOIA personnel. This 2025 update addresses new functionality available through the FOIA Search Tool that allows users to enter search terms to identify information that may be already publicly available or to identify the correct agency to submit a FOIA request if desired. This government-wide PIA addresses the use of NFP by public users and government personnel. Agencies maintain their own PIAs for agency-specific FOIA case management systems.

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.

NFP is a major application that consists of two main components: the public-facing web user interface where requesters can submit a request to any federal agency, and a backend site where the respective Agency Managers can update basic FOIA contact information for their agencies. The portal may connect to the respective agency FOIA websites via an API for purposes of sending the request to the

[1] Pub. L. No. 114-185, 130 Stat. 538 (codified at 5 U.S.C. § 552 (2018)).
[2] 5 U.S.C. § 552a. The primary purpose of the NFP is to serve as the consolidated online request portal for FOIA requests, as required by the FOIA Improvement Act of 2016. However, similar to traditional FOIA request processes, the NFP may also accept requests from an individual that may be processed under the Privacy Act's right of access provisions. Id. § 552a(d).

responding agency's separate FOIA website. The NFP connects to https://www.max.gov for purposes of Agency authorized user validation. Agency users authenticate into the site through https://www.max.gov by using either the Agency user's Personal Identity Verification (PIV) card or two-factor authentication. The responding agency's FOIA website, separate from the NFP, may connect to https://www.max.gov for purposes of Agency user identity verification.

The public-facing web user interface contains a FOIA Search Tool (www.foia.gov/wizard.html) where public user queries are sent to a separate machine-learning service hosted by a government contractor, Polydelta. This search feature helps public users locate the correct government agency to which they should submit their FOIA request and suggests publicly available records that may satisfy a public user's search query. Public users submit their query and receive suggestions from the FOIA Search Tool, while the data is passed to/from Polydelta in the background. While the FOIA Search Tool advises public users not to enter personally identifying information, some users may still do so. Certain types of personally identifiable information that are readily identified are automatically stripped via an automatic tool before they are processed by Polydelta. These data types include phone numbers, Social Security numbers, email addresses, IP addresses, driver's license numbers, Taxpayer Identification Numbers, and passport numbers. Names, place names, and dates are not stripped because they are generally relevant to a public user's query.

The FOIA Improvement Act of 2016 tasked the Director of the Office of Management and Budget, in consultation with the Attorney General, to ensure that the United States Government develops and operates "a consolidated online request portal that allows a member of the public to submit a request for records to any agency from a single website."[3] DOJ developed the NFP to comply with this requirement.

The type of information collected, maintained, used, or disseminated by the system include:

1) Public User Information Collected & Stored Automatically: When a public user visits NFP via its publicly-available website, the Department of Justice, or a contractor operating on DOJ's behalf, will automatically collect and store the following basic information: the name of the visitor's internet domain (for example, "xcompany.com" or "yourschool.edu"); the Internet Protocol (IP) address (a number that is automatically assigned to your computer when you are using the Internet) attributed to the public user at the time they visit NFP; the type of web browser and operating system; the date and time the public user visited the NFP site; the internet address of the website the public user used to travel directly to NFP; the pages the public user visits while using NFP; and the information the public user provides when making their requests. This information is collected, used, maintained, and disseminated in accordance with the DOJ Privacy Policy.[4]

2) Contact Information: For an agency to correspond with a public user, NFP requires public users to provide at least one form of contact information (indicated, below, by an asterisk (*)). The following fields are available to the requester via the NFP's FOIA Request function:

    - First Name (optional)

[3] *See id.* § 552(m)(1).
[4] https://www.justice.gov/doj/privacy-policy.

- Last Name (optional)
- Organization (optional)
- Email Address*
- Phone Number*
- Fax Number*
- Mailing Address*

3) "Your Request" Information: In addition, the public user must provide the description of the records sought. The description field is a free-form text field, which has a 10,000-character length maximum. The public user is directed immediately before they access the free-form text field to be specific and give agency FOIA personnel enough detail to be able to reasonably determine exactly which records are necessary to fulfill the request.

4) Requester type, Fees and Expedited Processing Information: The public user may also identify the requester type/category: "Representative of the news media;" "Educational Institution;" "Non-commercial scientific institution;" "Commercial-use requester;" or "All other requesters." Public users may also indicate whether they are making a request for fee waiver and provide fee waiver justifications and the amount of money the requester is willing to pay in fees to process the request, if any. Additionally, requesters may submit expedited processing requests and expedited processing justifications via a free-form text field.

5) "Upload Additional Documentation" tool: NFP provides an "Upload Additional Documentation" tool on each Agency's request form. A public user can use the tool to provide documents for the following purposes:

   a. To verify a public user's identity when they submit a request for records about themselves (a "first-party" request),
   b. Provide additional context for the user's request, which facilitates agency personnel's ability to process the request.

   File uploads are restricted to graphic interchange format (GIF),[5] joint photographic experts' group (JPEG),[6] portable network graphic (PNG),[7] printer definition file (PDF),[8] documents (DOC/DOCX),[9] open document format (ODF),[10] and text file types.

   Agencies are permitted to add additional fields to their respective NFP request forms to collect information that may be required by their FOIA regulations.

6) Federal Agency User Account Information: The NFP contains non-public federal agency user account information, including email addresses, usernames, passwords, and roles related to the

[5] GIF is an image file format commonly used for images on the web and sprites in software programs.
[6] JPEG is a standard image format for containing lossy data compression.
[7] PNG is a raster graphics file format that supports lossless data compression.
[8] PDF is a file format that provides an electronic image of text or text and graphics that looks like a printed image.
[9] DOC/DOCX is a Microsoft Word Open XML Format Document.
[10] ODF is an XML-based open source file format for saving and exchanging text, spreadsheets, charts, and presentations.

Agency Managers' Drupal accounts, which is managed and maintained by site administrators through authorized account access on NFP.

7) Agency Points of Contact Information: The NFP may also contain public point of contact information, including phone numbers, office mailing addresses, and email addresses. Those points of contact do not have access to the NFP, unless the point of contact also serves as the Agency Manager.

Via the public-facing frontend of NFP, members of the public can access the FOIA Search Tool and various agency-specific pages to submit requests to a designated agency. The public can also access "snapshot reports," which may provide, for example, the average processing time for the designated agency and a list of public-facing points of contacts for each agency.

Requesters submit information to an agency that they designate via the public facing NFP website, which sends the requests to the agency for ingestion into the agency's existing FOIA request tracking system. There are two methods for request delivery using the NFP: (1) via email to the designated agency; or (2) via an Application Programming Interface (API)[11] that is connected to the agency's FOIA case management system. Alternatively, requesters can use a link on the NFP website to the designated agency's own FOIA website which would allow the requester to submit a request in accordance with the designated agency's FOIA process. Upon receipt of the request, the designated federal agency is responsible for processing the request and responding directly to the requester, independent of the operation of the NFP. To process the request, personally identifiable information (PII) may be required so that the designated agency can correspond with the requester and otherwise process the request.

NFP also contains a FOIA Search Tool that allows users to identify the correct agency to submit their request and to identify information that may already be publicly available that would satisfy their query. The Search Tool includes pre-defined user journeys for common topics and a capability for users to enter their own search terms. Search Tool results are generated through a combination of logic-based and machine learning functionality. The results may provide explanatory information if a user enters a pre-defined user journey. Search results obtained outside a pre-defined user journey provide the titles of relevant documents and the name of the originating agency, along with one or more suggested agencies to submit a FOIA request. A machine learning service, connected to NFP via API, powers the document and suggested agency results. Document results are based on agencies' posted "frequently requested records." Suggested agency results are based on agencies' posted FOIA logs that provide information about the types of FOIA requests the agency has processed. For document results, NFP does not store the documents, but instead links to the documents posted on the agency's originating site. When the machine learning service ingests new documents (which does not happen automatically), it encodes the information necessary to generate results—underlying files are not stored.

[11] "Application Programming Interface" or "API" is a "system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality." NIST, Glossary: Application Programming Interface, https://csrc.nist.gov/glossary/term/Application-Programming-Interface.

On the backend of NFP[12], designated personnel in the Department of Justice (DOJ) Office of Information Policy (OIP), and Justice Management Division (JMD), Service Delivery Staff (SDS), Consolidated Web Services (CWS) team serve as the Administrators who are responsible for new account creation, user role management, systems maintenance, and administration functions. A DOJ Administrator manages request forms; creates and manages top level agencies by adding/editing/removing them; administers the onboarding and off boarding of agency components using the portal by creating and removing components in the system; makes necessary changes to the agency's component contacts who receive requests via the API; and manages the accounts for the Agency Manager. Within JMD SDS CWS, an Administrator provides site-wide administration with no permission restrictions. The DOJ OIP team personnel have access to the entire portal and all information within it, subject to access controls, discussed below.

Agency Managers have access to only their agency-specific information in NFP and must authenticate their identities via www.max.gov using a PIV or two-factor authentication.

Information is retrieved electronically via the NFP. The NFP supports three user types:

1) Public/Requesters: these users retrieve information from the system by visiting https://www.foia.gov or by submitting an API request to https://api.foia.gov within the NFP. No user account exists for this user in the backend/backstage.

2) Agency Managers: these users *curate* information saved in the NFP backend about their specific agency, logging in with a unique NFP account credential, and ensuring up-to-date agency contact information. Agency Managers do not have the capability to *retrieve* requester-furnished information from the NFP or from the backend site. Agencies respond directly to the requester upon notification from the NFP that a request has been received via an API connected to the agency's FOIA system (if present) or upon receiving an email notification from the NFP that a request has been submitted to the agency. The Agencies respond to the FOIA requester separately from FOIA.gov, via hard copy mail, fax, email, or other methods determined by the responding agency. There is at minimum one Agency Manager assigned per agency.

3) DOJ Administrators: these users, limited to DOJ OIP and JMD SDS CWS personnel, retrieve information from the system via command-line tools, dashboards, logs, and databases to ensure system maintenance and perform administrative functions. Audit log information about government employees authorized to perform backend updates may be retrieved by personal identifier.

The requester enters information directly to the NFP via a public facing web interface on FOIA.gov. Once the request is received into the NFP, there are two possible methods, which depend upon each agency's capabilities, for the requestor to request delivery: via email to the designated agency, i.e., the NFP will deliver the information provided by the requester in the NFP's data interface directly to a designated agency point of contact; or via an API that is connected to the agency's FOIA case

[12] The "backend" portion of NFP currently utilizes the Drupal content management system and is hosted by Acquia in Amazon Web Services.

management system. Alternatively, requesters can use a link on the NFP website to the designated agency's own FOIA website without inputting any information into the NFP. Upon receipt of the request by any of these methods, the designated federal agency is responsible for processing the request and responding directly to the requester, independent of the operation of the NFP.

The NFP collects, maintains, and disseminates requester information to the designated federal agency, allowing the agency to respond directly to a requester in accordance with the Freedom of Information Act, agency policy, and, if applicable, the Privacy Act. The agencies/components receive the requests via the NFP and will follow their specific agency/component procedures for fulfilling the requests; basic contact information collection and dissemination to the relevant agency is necessary for the agency to be able to appropriately respond to the requester or otherwise facilitate the request. Maintaining the collected information within the NFP on a temporary basis is necessary to ensure data integrity and normal system operation. DOJ uses website visitor information and analytics data to better understand usage of the NFP and identify areas for improvement, particularly of the FOIA Search Tool.

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	The Freedom of Information Act, 5 U.S.C. § 552 The Privacy Act of 1974, as amended, 5 U.S.C. § 552a
Executive Order	
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

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.

Agencies may require varying degrees of verification of requester identification, which may mean that some of these identification data may be provided through the NFP. Because this will vary agency to agency, the data points below that are marked with an 'X' represent the likely data points that will be submitted through the NFP. Agencies will not use the NFP to collect fees for processing requests;

therefore, the NFP does not collect requesters' financial information. Agencies may assign case identifiers to requests but will do so outside the NFP.

(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 and D	
Date of birth or age	X	A, B, C and D	
Place of birth	X	A, B, C and D	
Sex			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	A, B, C and D	
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address	X	A, B, C and D	
Personal phone number	X	A, B, C and D	
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			

(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			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			

(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
System admin/audit data:			
- **User ID**	X	A and B	
- **User passwords/codes**			
- **IP address**	X	A and B	
- **Date/time of access**	X	A and B	
- **Queries run**	X	A and B	
- **Contents of files**	X	A and B	
Other (please list the type of info and describe as completely as possible):	X	A, B, C and D	• ID Files Accessed • Federal agencies can customize the specific agency's FOIA request forms to require specific fields for their agency. While users are advised to enter information specific to their FOIA request, it is possible they may enter a variety of other unnecessary PII into the system's free text fields.

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		Online	X
Phone		Email			
Other (specify):					

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

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X

Commercial data brokers	X				
Other (specify):					

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			
DOJ Components			X	
Federal entities			X	
State, local, tribal gov't entities				
Public			X	Certain agency information, including point of contact information, may be publicly available at foia.gov.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector			X	CWS contractors.
Foreign governments				
Foreign entities				
Other (specify):				

The NFP will first share information with the agencies/components via direct access from the NFP to the respective Agency Managers; Agency Managers cannot retrieve request information from the NFP, i.e., they cannot query the NFP to locate a request using a requester's name or other identifying information. Agencies/components may further share the information described in section I (c), above, within the responding agency/component for purposes of responding to the requester. Depending on the nature of the request, the information may be shared within the agency/component, or larger disseminations of the information may be necessary to fulfill the underlying request—to include with other federal entities that may possess responsive records. Agency/component-specific processes will determine the extent of further information sharing; within the NFP itself, however, information is shared only with the Agency Managers and among the DOJ Site Administrators via direct access.

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 will not be released to the public for Open Data purposes.

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.

The NFP website is linked to the DOJ Privacy Policy, which outlines DOJ's requirements for collecting, storing, transmitting, and sharing information that is provided voluntarily through DOJ-affiliated websites. The notice is provided pursuant to a system of records notice published in the Federal Register.

For Agency Managers and DOJ Administrators, the system displays the following warning banner:

"You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties.

By logging in to this information system you are acknowledging that you understand and consent to the following:

- You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transiting or stored on this information system.
- Any communications transmitted through, or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

For further information see the Department Order on Use and Monitoring of Department Computers and Computer Systems."

For the public visiting foia.gov and providing information, a link to the DOJ Privacy Policy[13] is displayed at the bottom of all webpages. Additionally, the FOIA Search Tool specifically instructs users not to include their name, contact information, or other information that could be used to identify them.

[13] https://www.justice.gov/doj/privacy-policy

Additional notices and guidance are provided on the NFP website and allows the public to understand how information is collected, processed, and transmitted. This banner informs requesters on tips for making a request and actions taken by the designated federal agency upon the submission of the request. The FOIA Search Tool also explains to users how to construct their search queries and specifically instructs them to not include personally identifying information.

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.

The request for access to records is entirely voluntary, and individuals are not required to utilize NFP.

However, should an individual use the NFP to facilitate their request, the individual must provide the minimum information necessary to submit a request: a description of the records sought, the requester type, and at least one form of personal contact information to allow the designated federal agency to respond and correspond with the requester. The requester has the option to provide personally identifying information, *e.g.*, first and last names, and to upload attachments to the request, which may include additional personally identifiable information, but such information is not required in order to submit a request via the NFP.

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.

Submitting a request is at the discretion of the requester. If the requester is submitting a request for records on themselves (a "first party" request), they can use the NFP "upload additional documentation" function to attach documents to verify the requester's identity. This function can be used to upload any documents that provide context to the request or that could help FOIA personnel process the request. File uploads are restricted to GIF, JPEG, PNG, PDF, DOC/DOCX, ODF, and text file types.

Once information is submitted, individuals do not have the opportunity to consent to particular uses of the information. Rather the information will be used to further agencies' duties under the FOIA.

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):** 12/27/2023 – 12/27/2026 **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:** N/A
	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	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** Moderate
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Audit log analysis, continuous monitoring, and periodic security and privacy security control assessments.
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:** Audit logs include role-based access, web application logging, timestamp, source IP, and type of event.
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**.
X	**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:** General information security training, training specific to the system for authorized users within the Department, and training specific to the system for authorized users outside of the component.

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?

The following access and security controls have been utilized to protect privacy and reduce the risk of unauthorized access and disclosure:

- The NFP has a security categorization of FISMA Moderate. DOJ has assessed and implemented all applicable security controls that are the responsibility of DOJ for a FISMA Moderate baseline.
- The NFP backend system is accessible only to authorized users. Specifically, only the JMD SDS CWS and DOJ OIP designated personnel have administrative access to the back-end Drupal section of NFP. All other federal Agency Managers, who are responsible for maintaining contact information, can update contact information and basic information about their agency by using the authorized application login account.
- All DOJ users must complete Cybersecurity Assessment Training (CSAT) annually, as well as read and agree to comply with DOJ Information Technology Rules of Behavior, prior to accessing the backend NFP and annually thereafter.
- Audit logging is configured, and logs are maintained separate from other system data to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. JMD SDS CWS personnel will have access to the audit logs and account information for system maintenance and administrative functions.
- NFP is accessible utilizing tiered/role-based access. Agency Managers and DOJ Administrators log into the NFP via www.max.gov. MAX.gov can authenticate either through a PIV card or through another two-factor authentication method.

Additionally, Information Security Agreements (ISA), Memorandum of Understanding/Agreements (MOU/A), and cloud service provider contracts and agreements outline required safeguarding necessary to protect the information. In addition, OIP produces training information to the general public and federal agencies detailing the proper use of the NFP. Access controls are implemented to restrict access to authorized users, and audit logs are maintained that will associate a user to an action in the event an anomaly or incident is detected.

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.)

Once the request is sent to the designated agency (assuming that the agency is connected to the portal via an API), the content of the request is purged from the NFP backend interface immediately. If the agency is connected to the portal via email, the content of the request is retained by the NFP for seven days for auditing purposes. The fact that a request was transmitted to a particular agency, along with the time, date, method of transmission, and any error codes, is stored indefinitely in the NFP backend interface, while the substance of the request including any PII is purged immediately (if interoperable via API) or after 7 days (if interoperable via email). Generally, data is stored for two years in system backups (captured once every 24-hours) and by the recipient agency in accordance with the agency's records retention schedule. System backups generally will not include requests transmitted via API that are immediately purged upon successful transmission.

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).

__X__ No. _____ 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-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 Fed. Reg. 37188 (July 14, 2021); and
- JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, 77 Fed. Reg. 26,580 (May 4, 2012).

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?

Depending on the information provided by the public user of the NFP, the threats to individual privacy that could result from the inappropriate handling, retention, and disposition of, as compared to the collection of the NFP information include, but are not limited to, identity theft, blackmail, physical harm, discrimination, or emotional distress—particularly if personally identifiable information about a requester is improperly disseminated to persons without a need to know such information for purposes of processing the request.

Potential threats to privacy are informed by the information provided by each requester. Absent controls for the use and minimization of such information, threats to personal privacy in light of the type of information collected or its sources include revealing that a requester is participating in the request process, a requester's physical location (i.e., home address) or means to contact a requester (e.g., phone numbers and email addresses), and a requester's possible personal, professional, or commercial interests in the records sought. Risks of identity theft, blackmail, physical harm, discrimination, or emotional distress increase if the requester uploads sensitive personally identifiable information such as one's Social Security number or other identification number or biometric identifiers, medical information, criminal history, etc. Only basic identification information, e.g., full name, address, email, phone/fax numbers, is necessary from requesters seeking government records in order to appropriately respond to or otherwise facilitate requests. Therefore, the NFP requires the minimum amount of information—a valid contact method, a description of the records sought, and a requester type—in order to respond to the requester and to determine what if any fees might be assessed based upon the type of the requester, e.g., commercial use, educational institution use, etc. Agencies can require additional identifying information, and requesters have the option to upload attachments with the request, which may include Social Security numbers or other personally identifiable information (PII) that the requester decides to provide to the federal agency. The agency endpoints are required to start with hypertext transfer protocol secure (HTTPS), which means that

traffic to them uses secure sockets layer (SSL) encryption. The FOIA Search Tool discourages requesters from providing personally identifying information. If a user provides sensitive PII (such as a Social Security number) as part of their search query, this information will be scrubbed from any web analytics collected.

Potential threats to privacy are minimized by informing requesters of the types of information to be collected via the warning banner within the NFP, by limiting the identifying and contact information required, by limiting access to information to authorized users (only DOJ's OIP has the ability to retrieve the information in the NFP; the Agency Managers receive the requests in the NFP, which are delivered to their respective FOIA websites connected to the NFP via APIs; however, they cannot retrieve the requests directly from the portal), by ensuring encryption of data in transit and at rest, and by ensuring that information is removed from the system in a timely manner while complying with record retention schedules.

NFP transmits API requests (requesters information) through a HTTPS web browser connection, which means that traffic to them uses SSL encryption. The NFP database and file system is encrypted to provide additional protections to secure the information. If requests transmitted via email fail to send because they contain a Social Security number and are blocked by DOJ security tools, the DOJ administrators will manually encrypt and re-send the email.