Justice Management Division

Privacy Impact Assessment
for the
National Freedom of Information Act Portal

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

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: June 8, 2022

EXECUTIVE SUMMARY

The National Freedom of Information Act Portal ("NFP") 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 FOIA Improvement Act of 2016.[1] The information submitted in a Freedom of Information Act (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 because this system will maintain and collect 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 in order 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.

Section 1: Description of the Information System

(a) The purpose that the records and/or system are designed to serve:

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 NFP is a public-facing website that allows members of the public to submit requests for government records to any federal agency from a centralized web interface.

(b) The way the system operates to achieve the purpose:

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)[4] that

[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).
[3] *See id.* § 552(m)(1).
[4] "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.

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 requestor 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, deliver, or otherwise facilitate the requested records, accordingly.

(c) The type of information collected, maintained, used, or disseminated by the system;

1) Website Visitor Information Collected & Stored Automatically: When an individual accesses NFP via its publicly available website, the Department of Justice, or a contractor operating on behalf of the Department, 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) from which the visitor accesses the NFP site; the type of browser and operating system used to access the NFP site; the date and time the visitor accessed the NFP site; the internet address of the website from which the visitor linked directly to the NFP site; and the pages visited and the information requested (if any) within the NFP site. This information is collected, used, maintained, and disseminated in accordance with the DOJ Privacy Policy.[5]

2) Contact Information: In order for the agency to correspond with a requester, NFP requires requesters 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)
- Last Name (optional)
- Organization (optional)
- Email Address*
- Phone Number*
- Fax Number*
- Mailing Address*

3) "Your Request" Information: In addition, the requester must provide the description of the records sought. The description field is a free-form text field, which has a maximum 10,000-character length, and the requester is directed in instructions immediately preceding 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.

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

4) Fees and Expedited Processing Information: The requester 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." Requesters 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.

5) Additional Information: If the requester is submitting a request for records on themselves (a "first party" request), the requester 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 graphic interchange format (GIF),[6] joint photographic experts group (JPEG)[7], portable network graphic (PNG),[8] printer definition file (PDF),[9] documents (DOC/DOCX),[10] open document format (ODF),[11] 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 usernames, passwords, and roles related to the Agency Managers' Drupal accounts, which is managed and maintained by each Agency Manager 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 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.

(d) Who has access to information in the system;

Via the public-facing frontend of NFP, members of the public can access the various agency request submission requirements 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 points of contact in the agency's FOIA Office that do not have access to the NFP itself.

Agency Managers have access to only their agency-specific information in NFP and must authenticate their identities via www.max.gov.

---

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

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.

(e) How information in the system is retrieved by the user;

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 *receive* requester-furnished information from the system, 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 FOIA.gov website or from the backend site. Agencies respond directly to the requester upon notification within 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, fax, or mail from the requester. The Agencies respond 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 in order 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.

(f) How information is transmitted to and from the system;

The requester enters information directly to the NFP via a public facing web interface. Once the request is received into the NFP, there are two possible methods, which are dependent 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

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

interface directly to a designated agency point of contact; or via an API 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 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.

(g) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects);

The NFP 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 have access in order to 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 responding agency's separate FOIA website. The NFP connects to https://www.max.gov for purposes of agency validation. Agency users authenticate into the site through https://www.max.gov using either the user's Personal Identity Verification (PIV) card or unique user identification and password. The responding agency's FOIA website, separate from the NFP, may connect to https://www.max.gov for purposes of agency user identity verification.

(h) Whether it is a general support system, major application, or other type of system.

NFP is categorized as a major application.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated.

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.

Identifying numbers					
Social Security		Alien Registration	X	Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			

General personal data					
Name	X	Date of birth	X	Religion	

General personal data							
Maiden name		Place of birth	X	Financial info			
Alias		Home address	X	Medical information			
Gender		Telephone number	X	Military service			
Age		Email address	X	Physical characteristics			
Race/ethnicity		Education		Mother's maiden name			

Work-related data							
Occupation	X	Telephone number	X	Salary			
Job title		Email address	X	Work history			
Work address	X	Business associates					

Distinguishing features/Biometrics							
Fingerprints		Photos		DNA profiles			
Palm prints		Scars, marks, tattoos		Retina/iris scans			
Voice recording/signatures		Vascular scan		Dental profile			

System admin/audit data							
User ID	X	Date/time of access	X	ID files accessed	X		
IP address	X	Queries run	X	Contents of files	X		

Other information
Federal agencies are able to customize the specific agency's FOIA request forms to require specific fields for their agency.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	X
Telephone		Email			

Government sources					
Within the Component	X	Other DOJ components	X	Other federal entities	X
State, local, tribal		Foreign			

Non-government sources[13]					
Members of the public	X	Public media, internet	X	Private sector	X
Commercial data brokers	X				

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Potential threats to privacy are informed by the information provided by each requester. Absent controls for the use (see Section 3.5, below) 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

[13] FOIA requests may be submitted by any non-government source listed. The only data received would be the information provided in the FOIA requests.

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.

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), and by ensuring that information is removed from the system in a timely manner while complying with record retention schedules. Finally, Section 6.1 and 6.2 provides an overview of the security controls in place to prevent and mitigate the security threats that exist in light of the information collected, and the sources from which the information is collected.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): Since 1967, the Freedom of Information Act has provided the public the right to request access to records from any federal agency.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is

necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

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 cognizant agency is necessary in order 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 in order to ensure data integrity and normal system operation.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	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	
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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 request is retained by the NFP for seven days for auditing purposes, for two years in system backups, and by the recipient agency in accordance with the agency's records retention schedule.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic

purging of information in accordance with the retention schedule, etc.)

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 (see Section 2.3, above), 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.

Please refer to section I (d)-(h), above, discussing user access limitations and information retrieval and transmission. Additionally, NFP transmits requests through a Hyper Text Transfer Protocol Secure (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.

In addition, Section 6.1 and 6.2 provides an overview of the security controls in place to prevent and mitigate the threats associated with the unauthorized disclosure and compromise of privacy information.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component				
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
Private sector				
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 information from the NFP, *e.g.*, they cannot query the NFP in order 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 in order 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 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Requester information is transmitted through a secure Hyper Text Transfer Protocol Secure (HTTPS) web browser connection, which means that traffic to them uses SSL encryption. The NFP database and file system are both encrypted to provide an additional layer of protections.

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.

Section 6.1 and 6.2 provides an overview of the security controls in place to prevent and mitigate the threats associated with information sharing.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.

X	Yes, notice is provided by other means.	Specify how: 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[14] is displayed at the bottom of all webpages.
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: The request for access to records is entirely voluntary, and individuals are not required to utilize NFP.

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

		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.
	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Submitting a request is at the discretion of the requester. 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.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

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. Requesters are not required to provide any personally identifying information;

however, a lack of contact information and a designation of the type of requester making the request will limit the responding federal agency from processing the request and assessing fees, as appropriate. Once the requester submits information by filling out and submitting a form through the NFP, the designated federal agency will use that information to respond to the requester's message or to otherwise fulfill the stated purpose of the communication. Where feasible, the Department provides visitors with a notice at the point of collection when requesting personal information on Department websites, which may include a brief description of the Department's practices with respect to the collection, use, maintenance, or dissemination of personal information.

The Department maintains and disposes of personal information according to the requirements of the Federal Records Act, Department policies, and the regulations and records schedules approved by the National Archives and Records Administration. In some cases, the information the requester provides may be covered by the Privacy Act, or subject to the FOIA. Additionally, information referred to another agency by operation of the NFP may be subject to the records maintenance and related policies of the recipient agency.

Additional notices and guidance is 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.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: 1/8/2018
X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4.
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 DOJ's audit security standards. 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 provisions in their contract binding them under the Privacy Act.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.

X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
	X	Training specific to the system for authorized users within the Department.
	X	Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

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, responsible for maintaining contact information, have the ability to update contact information 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. Federal agencies logging into the NFP via www.max.gov. The Agency Manager and the DOJ Administrator have two (2) authentication methods; PIV or unique userid and password.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: • JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 FR 37188 (7-14-2021; and • JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, 77 Fed. Reg. 26,580 (May 4, 2012)
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information submitted by requesters can be retrieved online by authorized DOJ Site Administrators for seven (7) days, and in offline backups for two (2) years. Information can be retrieved via queries or unique request identifiers assigned by the system once the request is submitted in the NFP. The account, audit log, and user records maintained in this system to monitor system activity are covered by
JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 FR 37188 (7-14-2021)
In certain circumstances, a requester may request records from DOJ, which would be facilitated through DOJ's normal request process. In those circumstances, requester records may be part of JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records. Similarly, requests referred to other agencies by operation of the NFP would be subject to those agencies' respective SORN(s).