Office of Information Policy

Privacy Impact Assessment
for
OIP's Use of FOIAonline

Issued by:
Senior Component Official for Privacy,
Carmen Mallon, Chief of Staff

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

Date approved: [July 12, 2017]

(May 2015 DOJ PIA Form)

Blank Page

EXECUTIVE SUMMARY

FOIAonline is a web-based application that facilitates acceptance, tracking, processing, and reporting of public requests to the Office of Information Policy (OIP). FOIAonline developed through a voluntary partnership of federal agencies as a comprehensive, centralized case management solution to facilitate implementation of the Freedom of Information Act (FOIA). FOIAonline allows for the submission, tracking, and case management of FOIA requests, Privacy Act of 1974 ("Privacy Act") requests, and FOIA and Privacy Act administrative appeals. FOIAonline also allows for the case tracking of Mandatory Declassification Review requests, Presidential Records Act requests, inquiries submitted to OIP regarding federal agency compliance with the FOIA, Executive Secretariat matters including congressional mail regarding requests or appeals handled by OIP, and FOIA litigation. FOIAonline also serves as an electronic records management system. Specifically, FOIAonline stores FOIA requests and appeals, records responsive to requests, notes, and correspondence related to requests and appeals, appeal background information, and OIP's responses to requests and appeals. FOIAonline interfaces with the Department's Federated Services authentication system. FOIAonline also interfaces with Pay.gov,[1] which allows requesters to pay their fees online.

OIP conducted a Privacy Impact Assessment (PIA) for FOIAonline because FOIAonline maintains and collects information about FOIA and Privacy Act requesters who submit requests and appeals to OIP. Members of the public can submit their requests using FOIAonline. Requesters may also submit requests and appeals by mail, fax, or email. OIP then manually enters the requests or appeals into FOIAonline for tracking purposes. Requesters provide their contact information and, for requesters seeking information about themselves, a certification of identity as required by Department regulations. Although FOIAonline is a shared government solution managed by the U.S. Environmental Protection Agency (EPA) and used by several agencies, this PIA is limited to OIP's use of FOIAonline.

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

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

OIP oversees the Department of Justice's obligations under the FOIA. OIP adjudicates administrative appeals from denials of access to records made 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, and Associate Attorney General, as well as other Senior Management Offices; provides staff support for the Department Review Committee, which reviews Department of Justice 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

[1] More information on pay.gov is available at: https://pay.gov/public/home.

handles the defense of certain FOIA matters in litigation. FOIAonline will assist OIP in executing these responsibilities effectively and efficiently.

(b) The way the system operates to achieve the purpose(s);

FOIAonline developed through a voluntary partnership of federal agencies as a comprehensive, centralized case management solution to facilitate implementation of FOIA. FOIAonline allows for the submission, tracking, and case management of FOIA requests, Privacy Act requests, and FOIA and Privacy Act administrative appeals. FOIAonline also allows for case tracking of Mandatory Declassification Review requests, Presidential Records Act requests, inquiries submitted to OIP regarding federal agency compliance with the FOIA, Executive Secretariat matters including congressional mail regarding requests or appeals handled by OIP, and FOIA litigation.

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

The system collects information necessary to respond to FOIA requests and appeals sent to OIP. The information may include: name, address, email address, telephone number(s), prison registration number, Social Security number (SSN), and job title. The pieces of information collected depend on the information provided by the requester, and the information required by regulation for processing the request. FOIAonline does not specifically ask requesters to provide their SSNs; however, a requester may voluntarily provide it as part of the requester's certification of identity.

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

Approved users within OIP have access to the information within the system. Approved OIP users enter information into the system and may retrieve information by searching any of the information fields. EPA manages and hosts FOIAonline. Accordingly, EPA's development contractors have access to all the OIP information in the system, including information about OIP users and other substantive information contained in the system, for the purposes of system administration and enhancement.

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

In most cases, OIP searches by the request or appeal number assigned to the case. OIP may also search using other search terms, such as the requester's name, the request description, or the date of the request.

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

Information is transmitted to and from the system using the FOIAonline web application. There is a public-facing request portal that requesters use to submit requests or appeals. Requesters may choose to set up a FOIAonline account that they access with a username (email) and password. This allows them to submit requests and appeals using FOIAonline,

correspond with OIP, and view OIP's responses by logging onto the system. Requesters may also submit requests or appeals through FOIAonline without creating an account. In that case, OIP emails its response to the requester rather that providing it through the FOIAonline application. Finally, requesters may submit requests and appeals by mail, fax, or email. In these cases, OIP manually enters the request or appeal information into FOIAonline for tracking. OIP provides its responses to the requester via email or mail, depending on the requester's preference.

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

FOIAonline interfaces with the Department's Federated Services authentication system. This allows OIP users to access FOIAonline using dual factor authentication with their personal identity verification (PIV) cards. FOIAonline also has the capability to interface with Pay.gov, which allows requesters to pay their fees online. OIP rarely assesses fees, so EPA has not yet configured this capability. If EPA does configure it in the future, requesters could access Pay.gov through FOIAonline to pay any applicable fees online. Requesters may also submit payments by mail.

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

FOIAonline is a major application that provides requesters with the capability to submit requests and appeals to OIP online, facilitates OIP's communications with requesters who have FOIAonline accounts, and allows OIP to track all requests and appeals received.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

In processing requests and appeals, OIP uses FOIAonline to collect, maintain, or disseminate: requester name, alias, home address, telephone number, email address, file/case ID numbers, and work-related contact information for business representatives or attorneys representing requesters. FOIAonline does not require individuals to provide their SSNs, but some requesters may voluntarily provide their SSNs in their request. The Department's Certification of Identity Form 361[2]—developed to assist an individual in verifying his or her identity for requests under the Privacy Act and the FOIA to ensure that records about individuals are not wrongfully disclosed—includes the SSN as an optional piece of information that requesters can provide to assist the agency in locating records about them. FOIAonline creates a unique tracking number for each matter entered into the system. When OIP enters new information into the system, FOIAonline automatically generates the tracking number, which identifies the matter as a request or appeal, indicates the fiscal year in which the requester

[2] DOJ Form 361 is available at: https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/cert_ind.pdf.

submitted the request or appeal, and includes a number that allows OIP to distinguish the request or appeal from others received in the same fiscal year. OIP provides the requester with the tracking number in the acknowledgment letter and references the tracking number in all communications with the requester.

The system's audit log compiles the date and time of each user's system access and the specific files accessed. User ID's are maintained as part of each user's profile and may only be edited by a system administrator. EPA maintains and monitors the audit logs as part of its administration of FOIAonline, and OIP can request access to audit logs as needed.

Additionally, FOIAonline will retain all final responses for FOIA and Privacy Act requests, 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 FOIAonline 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 FOIAonline. Therefore, the items of information checked below are limited to FOIAonline user account information, log information, and the information collected, maintained, or disseminated to process requests and appeals handled by OIP.

Identifying numbers					
Social Security	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID	X	Credit card			
Other identifying numbers (specify): Although OIP does not require prisoners to provide their prison registration numbers, a prisoner may provide a registration number to confirm proper identification. The prisoner number will then become part of the contact information for future OIP correspondence.					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth	X	Financial info	
Alias	X	Home address	X	Medical information	
Gender		Telephone number	X	Military service	
Age		Email address	X	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify): FOIAonline provides an opportunity for a requester or appellant to create a user account. The user account permits the requester or appellant to submit a request or appeal online, and receive status updates and OIP's response through email. Requesters and appellants may submit a request or appeal through FOIAonline without creating an account, but they must provide a mailing address. If requesters or appellants do not provide their email addresses, the requester will receive their response by mail.					

Work-related data					
Occupation		Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates			
Other work-related data (specify):					

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

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address		Queries run		Contents of files	
Other system/audit data (specify): EPA contractors monitor audit logs as part of regular security controls. OIP can request access to audit log information from EPA as needed.					

Other information (specify)
FOIAonline 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 FOIAonline 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 FOIAonline.

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

FOIAonline collects information directly from individuals, their representatives, and from other DOJ components and other federal entities.

FOIAonline may collect general personal data and work-related data about a requester from other DOJ components and federal entities if records responsive to a request received at the other component or entity either originated with, or are of particular interest to, OIP or one of the Department of Justice's Senior Leadership Offices. The other component or entity will generally refer the records to OIP for processing and response to the requester. Similarly, another component or entity may consult with OIP to determine the appropriate response to a request if the responsive records contain equities belonging to OIP or one of the Department's Senior Leadership and/or Management Offices. Another component or entity may route a misdirected request to OIP if it determines that OIP or the Senior Leadership Offices are the components to which the requester intended to send the request. In these situations, OIP

receives the general personal data and work-related data required to respond to the request.

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax	X	Online	X
Telephone	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		Other DOJ components	X	Other federal entities	X
State, local, tribal		Foreign			
Other (specify):					

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify):					

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.)

The risks associated with the collection of data in the FOIAonline system include unauthorized access to the system and compromise of data by an internal user. FOIAonline is a system owned by the federal government and hosted by the EPA. As a result, OIP does not directly oversee the system itself.

Consistent with the Memorandum of Agreement between the EPA Office of Information Collection and OIP, EPA is the program manager of FOIAonline. EPA uses contracted developers for system development and support. OIP is a co-chair of the FOIAonline interagency governance board, made up of the EPA and FOIAonline partner agencies. Although many agencies use FOIAonline, the system is set up with strict access controls such that only EPA, as program manager of the system, can access other agencies' data. The contracted developers that EPA manages can access OIP's data to enhance and maintain the system.

FOIAonline also shares its infrastructure with the government-wide eRulemaking system, hosted at the National Computer Center in Research Triangle Park, North Carolina. Although EPA manages the system, OIP has implemented a number of protections to mitigate the risk of unauthorized access. Access to FOIAonline requires an agency user to authenticate through DOJ's Federated Services using his or her PIV card. EPA contractors also review audit logs that track use of the application, and regularly use this technique to detect unusual activity indicating a potential compromise of the information. OIP can request access to audit logs as well. Finally, users have appropriate access to information based upon least privilege, and a user may only access the amount of information needed to perform his or her job function. All users must read, sign, and conform to the Rules of Behavior, which hold users accountable for appropriate use of the information accessible through FOIAonline

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
X	For litigation		
	Other (specify):		

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.

OIP oversees DOJ's obligations under the FOIA. OIP adjudicates FOIA and Privacy Act administrative appeals that the Department receives; processes FOIA and Privacy Act initial requests for records of the Offices of the Attorney General, Deputy Attorney General, and Associate Attorney General, as well as other Senior Management Offices; provides staff support for the Department Review Committee, which reviews Department of Justice 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.

To fulfill these functions and respond to requests from the public, OIP must collect information to correspond with a requester concerning the requester's FOIA request, Privacy

Act request, or administrative appeal. For Privacy Act requests, OIP collects information to verify the requester's identity before releasing information. FOIAonline also permits tracking of other types of requests that OIP processes, including Mandatory Declassification Review requests, Presidential Records Act requests, and inquiries submitted to OIP regarding federal agency compliance with the FOIA. OIP manually enters information about these other types of requests into FOIAonline for tracking purposes only. The public neither submits nor receives responses to these other requests through FOIAonline, nor are these final responses retained in FOIAonline.

OIP may share information with United States Attorneys' Offices or the Civil Division of the Department of Justice if the request becomes the subject of litigation. OIP may also share information with other Department of Justice components or federal entities if records responsive to a request to OIP contain information requiring consultation with or referral to the other component or entity. Finally, OIP may share information with the Office of Government Information Services (OGIS) of the National Archives and Records Administration (NARA) to the extent necessary to fulfill its responsibilities under 5 U.S.C. § 552(h), to review administrative agency policies, procedures, and compliance with the FOIA, and to facilitate OGIS's offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies.

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	5 U.S.C. § 552, the Freedom of Information Act 5 U.S.C. § 552a, the Privacy Act 44 U.S.C. § 2201, Presidential Records Act
X	Executive Order	Exec. Order No. 13,526, 3. C.F.R. 298 (Dec. 29, 2009)
X	Federal Regulation	28 C.F.R. Part 16; 28 C.F.R. Part 17
X	Memorandum of Understanding/agreement	Memorandum of Agreement between U.S. Environmental Protection Agency Office of Information Collection and U.S. Department of Justice Office of Information Policy
	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.)

Records maintained in FOIAonline are retained and disposed of in accordance with record retention schedules approved by the National Archives and Records Administration.

(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.

FOIAonline contains an internal management feature that categorizes information based on the appropriate records retention schedule. When the retention period ends for a particular piece of information, the system alerts the administrator that the retention period has ended. At that time, the system administrator can authorize deletion of the information. The system administrator augments FOIAonline with Documentum, a records management program that facilitates proper records retention.

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.)

OIP limits the use of personal and work-related data to communications with requesters who provided the data. Any privacy threats posed by OIP's use of the data would arise based on circumstances addressed in Section 2.3. Specifically, the risks to retaining data in the FOIAonline system include unauthorized access to the system and compromise of the data by an internal user.

The FOIAonline system employs two-factor authentication and role-based access controls to ensure data is handled, retained, and disposed of appropriately. The authentication controls require each user to access the system through DOJ's Federated Services using their PIV card and PIN. The role-based access controls allow the system administrator to grant access to information based on a least privilege access setting. In addition to this least privilege access system, FOIAonline users must read and sign a Rules of Behavior agreement before the administrator creates the user's account. The Rules of Behavior agreement holds each user accountable for appropriate use of the information stored in FOIAonline, including using information for official business only and protecting confidentially sensitive information from unauthorized disclosure. The system administrator creates and cancels accounts as part of the new hire and exit process. Additionally, all users must complete annual Department security awareness training.

Finally, the FOIAonline system creates an audit log of the application. The system administrator regularly reviews the log to detect unusual activity indicating a potential compromise of 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			X	
DOJ components	X			
Federal entities	X		X	EPA, for the limited purpose of administering FOIAonline.
State, local, tribal gov't entities				
Public	X			
Private sector			X	EPA's system management contractors, for the limited purpose of administering FOIAonline.
Foreign governments				
Foreign entities				
Other (specify):				

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.)

OIP may share the information collected in FOIAonline on a case-by-case basis in order to respond to a request or an appeal. For example, if OIP locates records in response to a request in which another agency or component has an interest, OIP may consult with the other agency/component before making a release determination, or OIP may refer those records to the other agency/component for direct response to the requester. OIP would share the requester's contact information with the other agency to facilitate their direct response to the requester. Additionally, in processing administrative appeals, OIP may share information about the appeal with the component that processed the initial request to gather background information or require further work on the request. OIP shares information on a need-to-know basis only, and may share information via email, mail, facsimile, or phone in accordance with Department policies. When shared within the Department, other components are required to conform to Department policies to prevent or mitigate threats to privacy through disclosure, such as

maintaining the integrity of their FOIA tracking application.

EPA's system management contractors for FOIAonline have access to OIP's data for system maintenance and enhancement. All users are responsible for protecting the privacy rights of requesters and receiving appropriate training. The Memorandum of Agreement outlines OIP's use of FOIAonline and identifies EPA and OIP responsibilities, which provides that EPA maintain the FOIAonline security plan.

FOIAonline is a FISMA moderate system that complies with National Institute for Standards and Technology (NIST), Special Publication 800-53, Revision 4, requirements and associated controls. Each agency's information is restricted to its agency's users unless otherwise made public. OIP will perform work using two-factor authentication. FOIAonline employs role-based access controls to ensure data is handled, retained, and disposed of appropriately.

Additionally, through training, OIP trains individuals on redaction processes and procedures to prevent the unauthorized disclosure of information. OIP staff members redact sensitive information from all documentation prior to disclosing. Additionally, OIP staff members must take Cyber Security Awareness Training annually and sign the DOJ Rules of Behavior.

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: The FOIAonline website includes a privacy and security notice that informs requesters of the information collection. Users may link to the notice at the bottom of the page, and users with accounts receive notice when they log in.
	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: FOIAonline is an optional service through which individuals may submit FOIA or Privacy Act requests. Individuals may also submit FOIA or Privacy Act requests via mail, fax, or email, and OIP manually enters this information into FOIAonline for

		tracking purposes. An individual is not required to file a FOIA or Privacy Act 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 seeking records about himself/herself 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 FOIAonline 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 a mailing address in order to receive a response from OIP. A person seeking records under the Privacy Act who does not provide adequate identifying information under 28 C.F.R. § 16.41(d), will only receive information under the FOIA.
	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: By submitting a proper FOIA or Privacy Act request, administrative appeal, or other request that utilizes FOIAonline, an individual provides information in order for OIP to respond to the request or appeal. OIP maintains this information in FOIAonline, whether the requester uses FOIAonline to submit their request or OIP manually enters the request information into FOIAonline. If an individual does not provide the requested information, OIP cannot respond. Applicable

		provisions of the Privacy Act and System of Records Notices, however, limit the use of the information.

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.

Individuals are provided clear and conspicuous notice through a Department-wide System of Records Notice, described in Section 7, a Privacy Act Statement that appears on the Department's Certification of Identity Form 361, and through the privacy and security notice that appears on the FOIAonline website. An individual is not required to file a FOIA or Privacy Act request, but if an individual 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 seeking records about himself/herself does not provide the appropriate certification of identity. OIP is unable to respond to any requester that does not provide adequate contact information. If a requester or appellant uses FOIAonline to communicate with OIP, then the requester or appellant could decline to provide some general personal data or work related data. The requester or appellant, however, would need to provide a mailing address in order to receive a response from OIP. Individuals do not have an opportunity to consent to particular uses of the information; however, applicable provisions of the Privacy Act and System of Records Notices limit the use of the information.

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: December 11, 2015 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
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: FOIAonline is a FISMA moderate system that complies with NIST 800-53 Rev. 4 requirements and associated controls.

X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: EPA is responsible for maintaining the FOIAonline security plan and conducts monitoring, testing, and evaluation necessary to fulfill security requirements.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Audit logs tracking use of the application are reviewed regularly to detect unusual activity indicating a potential compromise of the information. Users have appropriate access to information based upon least privilege and must read, sign, and conform to the Rules of Behavior, which hold users accountable for appropriate use of the information accessible through FOIAonline.	
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.
		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.

As discussed in Sections 2.3 and 3.5, OIP has implemented a number of protections to mitigate the risk of unauthorized access. Pursuant to the Memorandum of Agreement between OIP and EPA, EPA manages FOIAonline and is responsible for maintaining security controls. FOIAonline is a FISMA moderate system. EPA hosts the system on the same infrastructure as the government-wide eRulemaking system. EPA system managers regularly review audit logs tracking use of the application to detect unusual activity indicating a potential compromise of the information. In addition to EPA's management of the system, OIP further mitigates risks to privacy. OIP users access FOIAonline through dual-factor authentication using their PIV cards and PIN. Finally, users have appropriate access to information based upon least privilege and must read, sign, and conform to the Rules of Behavior, which hold users accountable for appropriate use of the information accessible through FOIAonline.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created, or has been 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-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, 77 Fed. Reg. 26,580 (May 4, 2012); • EPA/GOVT -002, Federal Docket Management System (FDMS) (EPA-GOVT-2), 78 Fed. Reg. 60,868 (Oct. 2, 2013)
	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.

FOIAonline permits retrieval of information based on the individual's name, the tracking number OIP assigned to the matter, the subject matter, or date of the request.