Office of Information Policy

Privacy Impact Assessment
for
eFOIA

Issued by:

Carmen Mallon, Chief of Staff

Reviewed by: Luke J. McCormack, Chief Information Officer, Department of Justice

Approved by: Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: June 27, 2012

(February 2011 DOJ PIA Form)

Section 1: Description of the Information System

The eFOIA System is a web-based, commercial off-the-shelf application for tracking, processing, and reporting for requests from the public received by the Office of Information Policy (OIP). The matters tracked by the system include: Freedom of Information Act (FOIA) requests; Privacy Act requests; Freedom of Information Act and Privacy Act administrative appeals; Mandatory Declassification requests; Presidential Records Act requests; inquiries submitted to OIP regarding federal agency compliance with the FOIA; Executive Secretariat matters, such as congressional mail regarding requests or appeals handled by the Office; and FOIA litigation. The system collects information necessary to respond to these matters. The information collected may include: name, address, email address, telephone number(s), prison registration number, 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.

Only approved users within OIP have access to the information compiled in the system. Information is entered into the system by an approved OIP user and may be retrieved by searching any of the information fields. In most cases, OIP searches by the requester's name.

The eFOIA system does not connect with any other systems; therefore, information is not transmitted to or from another system.

Section 2: Information in the System

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

Identifying numbers					
Social Security		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): The eFOIA system creates a unique tracking number for each matter entered into the system. The requester is provided the tracking number and the tracking number is referenced in all communications with the requester.

Although a prisoner's registration number is not a required field of information collected by OIP, a prisoner may provide a registration number as a method to confirm proper identification and is included as part of the contact information when corresponding with a prisoner.

General personal data

General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		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): Only general personal data provided directly by an individual is collected in eFOIA.

OIP's online request and appeal submission portal provides an opportunity for a requestor or appellant to create a user account. The user account permits the requester or appellant to submit a request or appeal online, receive status updates and OIP's response through email. If a requester or appellant chooses to use an online account, an email address is required.

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): Work-related data is collected when a request is made by a representative of a business, or by an attorney representing a client. Work-related data is limited to information required to correspond with the requester or appellant.

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): eFOIA does not collect "Distinguishing features/Biometrics" data.

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): The system's audit log compiles the date and time of each user's access and the files the user accessed. User ID's are maintained as part of each user's profile and may only be edited by a system administrator.

Other information (specify)

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	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): eFOIA collects 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 originated with OIP or one of the Department of Justice's Senior Leadership Offices. The other component or entity may refer the records for OIP's response. 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 Offices. Another component or entity may route a misdirected request to OIP if it determines that OIP or the Senior Leadership Offices are the agency to whom 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.					

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify): eFOIA does not collect general personal data or work-related data from a non-government source.					

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 to data in the eFOIA system include unauthorized access to the system and compromise of the data by an internal user. OIP has implemented a number of protections to mitigate the risk of unauthorized access. The system is hosted on Enterprise Solutions Hosting Platform (ESHP), which is supported by System Development Services (SDS) and Operations Solutions Staff (OSS). OSS maintains the firewall and intrusion detection system which protects the security boundary from unauthorized access. Audit logs tracking use of the application are reviewed regularly to detect unusual activity indicating a potential compromise of the information. 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 eFOIA.

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 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 Privacy Act; 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.

In order to fulfill these functions by responding to requests from the public, OIP must collect information to correspond with a requester concerning the requester's FOIA request, Privacy Act request, administrative appeal, Mandatory Declassification Review request, Presidential Records Act request, or inquiry submitted to OIP regarding federal agency compliance with the FOIA. For Privacy Act requests, the information collected also is used to verify the requester's identity before releasing information.

Information may be shared with United States Attorneys' Offices or the Civil Division of the Department of Justice if the request becomes the subject of litigation. Information may be shared 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.

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. § 16-17
	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.)

Records maintained by eFOIA are retained and disposed of in accordance with record retention schedules approved by the National Archives and Records Administration (NARA). NARA's General Records Schedule (GRS) 14, Information Services Records, controls the retention and destruction of records pertaining to information services functions performed by agencies, including the FOIA, Privacy Act, and Mandatory Declassification 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 14, request and appeal records may be retained for a maximum of six years; litigation records are retained for ten years.

The eFOIA system contains an internal management feature which 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.

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.

The eFOIA system employs authentication and role-based access controls to ensure data is handled, retained, and disposed of appropriately. The authentication controls require each user to utilize a user name and strong password based on specifications required by the Department of Justice. Password controls prompt users to create a new password on a regular basis and require the user to create a strong password. 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, eFOIA 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 the eFOIA system. The system administrator creates and cancels accounts as part of the new hire and exit process. In addition to these protections, all users are required to complete annual security awareness training sponsored by the Department.

Finally, the eFOIA 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	

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities				
Public	X			
Private sector				
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 eFOIA on a case-by-case basis in order to respond to a request or an appeal. Information is shared on a need-to-know basis only. When shared within the Department, other components are required to conform to departmental policies to prevent or mitigate threats to privacy through disclosure, such as maintaining the integrity of its FOIA tracking application.

OIP implements FISMA security controls as mandated in FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," and augmented in NIST SP 800-53, "Recommended Security Controls for Federal Information Systems." OIP implementation of these controls and associated risks and mitigation is reflected in FISMA and DOJ Order 2640.2F "Information Technology Security" mandated documentation.

Through access enforcement, the information system enforces approved authorizations for logical access to the system. Access enforcement mechanisms are employed to control access between users and eFOIA files, records, processes and programs in the information system. In addition to enforcing authorized access at the information- system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Additionally, all actions require identification and authentication.

Through boundary protection, OIP physically allocates publicly accessible information system components to separate subnetworks with separate network interfaces.

Additionally, through training, OIP ensures that FOIA responses do not contain nonpublic information.

OIP trains individuals on redaction processes and procedures to prevent the unauthorized disclosure of information. OIP staff redact sensitive information from all documentation prior to releasing. OIP staff additionally are required to 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.	
	Yes, notice is provided by other means.	Specify how:
	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: A requester may decline to provide information by not responding to a notice from OIP that the request does not comply with regulations. However, OIP is unable to respond to any requester that does not provide adequate contact information. If a requester or appellant uses the online portal 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 need to provide an email 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 the eFOIA system, an individual provides the information in order for OIP to respond to the request or appeal. If an individual does not provide the requested information, OIP cannot respond.

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 do not have an opportunity to consent to particular uses of the information. However, use of the information is limited by applicable provisions of the Privacy Act and System of Records Notices.

Section 6: Information Security

6.1 Indicate all that apply.

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: eFOIA has a C&A, which is located in CSAM, which includes all security controls that were tested, all artifacts, and all risk reports and other documentation, in the System Security Plan and Security Assessment Report.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: the eFOIA has auditing analysis and review which is done by OIP for the application and by SDS for the database and software and OSS at the network and operating system level to monitor, test and evaluate the information contained in eFOIA and prevent its misuse. eFOIA is hosted on ESHP, which is supported by SDS and OSS.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: March 2012	
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: the eFOIA has auditing analysis and review which is done by OIP for the application and by SDS for the database and software and OSS at the network and operating system level to monitor, test and evaluate the information contained in eFOIA and prevent its misuse. eFOIA is hosted on ESHP, which is supported by SDS and OSS.	
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. The system is hosted on Enterprise Solutions Hosting Platform (ESHP), which is supported by System Development Services (SDS) and Operations Solutions Staff (OSS). OSS maintains the firewall and intrusion detection system which protects the security boundary from unauthorized access. Audit logs tracking use of the application are reviewed regularly to detect unusual activity indicating a potential compromise of the information. 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 eFOIA.

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: Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records (DOJ-004), 77 Fed. Reg. 26580 (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.

eFOIA permits retrieval of information based on the individual's name or the tracking number OIP assigned to the matter.