Office of the Pardon Attorney

Privacy Impact Assessment
for the
Electronic Clemency Records Database

Issued by:
Ronald L. Rogers
Pardon Attorney

Reviewed by: Vance E. Hitch, Chief Information Officer, Department of Justice

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

Date approved: September 19, 2011

(February 2011 DOJ PIA Form)

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;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system; and
(g) any interconnections with other systems.

(a) ECRD is a database engineered to serve as the primary record for presidential clemency applications from initial application to adjudication by the President and final disposition.
(b) Through a variety of inputs and attached documents, case files will exist electronically as workflows within ECRD. Evaluations and recommendations will be recorded in and/or attached to workflows. The database will facilitate the use of various pieces of information to ease the processes of generating/responding to correspondence, generating statistical reports, and aiding in the evaluation of cases.
(c) Information maintained within the system will relate to a petitioner's federal conviction and accompanying obligation (be it imprisonment, restitution, supervised release, etc.). Some personal information like SSN, DOB, BOP register number, and FBI number will be maintained in ECRD. Also, ECRD will contain notes and recommendations derived from the deliberative process of OPA staff.
(d) Access to the system is limited to the staff of OPA.
(e) Users may access a workflow by looking up any identifying personal information. This includes but is not limited to: name, BOP register number, FBI number, and SSN.
(f) Some data will be manually entered by OPA staff into user-defined fields (UDFs). This manually entered data will originate from reports run in BOP Sentry (and other official sources) and notes and recommendations derived from the deliberative process of OPA staff. Court and prison documents which detail a petitioner's federal conviction, sentence, and fulfillment of sentence will be electronically attached to workflows and accessible from within the system. Any documentation related to a petitioner's case that is received by OPA in paper form will be scanned and electronically attached to the corresponding workflow (this includes but is not limited to: application and related correspondence). Finally, a web service will connect ECRD to OneDOJ. This one-way connection will allow OneDOJ to automatically populate fields related to a petitioner's federal conviction, sentence, and fulfillment of sentence.
(g) A web service will connect ECRD to OneDOJ. This one-way connection will allow OneDOJ to automatically populate fields related to a petitioner's federal conviction, sentence, and fulfillment of sentence.

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	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): FBI Number; BoP Register Number					

General personal data					
Name	X	Date of birth	X	Religion	X
Maiden name	X	Place of birth	X	Financial info	X
Alias	X	Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service	X
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X	Education	X	Mother's maiden name	
Other general personal data (specify): Children with date and place of birth, marriage history					

Work-related data					
Occupation	X	Telephone number	X	Salary	
Job title	X	Email address		Work history	X
Work address	X	Business associates	X		
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	X	Queries run	X	Contents of files	X
Other system/audit data (specify):					

Other information (specify)
Credit report/information; federal convictions: offense, sentence, district, date; Transmittal response dates; recommendation; grant/denial with date.

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

Directly from individual about whom the information pertains

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

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

Non-government sources					
Members of the public	X	Public media, internet	X	Private sector	X
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.)

We will retain such personal identifying information as SSN, BOP register number, and FBI number. These numbers are the main avenues through which we can manually look up a person's federal conviction(s) and sentence(s). These numbers are also the way we use the web service connection with OneDOJ to pull in information regarding a person's federal conviction(s) and sentence(s). We communicate with petitioners who are not incarcerated directly, so we maintain their home address/other relevant contact information. Personal data like mother's maiden name, as well as work data, are needed to verify that the information provided by a petitioner is accurate. We will not maintain any distinguishing features/biometrics in ECRD. In general, all data obtained from sources other than the petitioner himself is so obtained to ensure accuracy; the eventual recommendation produced by OPA, and ultimately reviewed by the President, is based upon much of this basic information.
System audit data will track each staff member, what data he accesses within ECRD, when he accesses that data, and for how long. By keeping constant track of who views what data, we limit security risks.

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		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): To conduct analysis in the processing of presidential clemency applications.		

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 information that maintained in ECRD is needed to help provide the basis for an informed judgment about whether clemency is warranted. OPA will use all information gathered to author a recommendation which will ultimately be reviewed and adjudicated upon by the President.

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	Title 28 United States Code (U.S.C.) Sections (§§) 533, 534; the Uniform Federal Crime Reporting Act of 1988, Public Law 100-690, Title VII, Subtitle I, § 7332 (codified as a note to section 534); Title 28 Code of Federal Regulations § 0.85.
X	Executive Order	Executive Order of the President No. 11878 (published at 40 FR 42731), as delegated by the Attorney General to OPA in 28 CFR 0.35 and 0.36 (Attorney General Order No. 1012-83, as amended at 65 FR 48381 and 65 FR 58223, published at 48 FR 22290), and as described in 28 CFR 1.1 through 1.11 (Attorney General Order No. 1798-93, published at 58 FR 53658).
	Federal Regulation	44 U.S.C. § 3101.
	Memorandum of Understanding/agreement	

X	Other (summarize and provide copy of relevant portion)	United States Constitution, Article II, section 2, to the DOJ in Executive Order of the President 30-1, dated June 16, 1893.

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.)

Information will be retained within ECRD for 15 years after the year the case is adjudicated upon. After this period, records will be accessed to NARA and the records will be deleted from the system and destroyed. A 15 year retention period fulfills our business need of reference. This records schedule is pending approval, Job Number N1-204-08-001.

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.)

Potential threats to privacy are most directly related to willful misuse of personal information. To this end, OPA will have mandatory training for all system users so they know how to deal with sensitive personal information before ECRD goes live, and for any new users before they may gain access to the database. Information will be purged from the system after 15 years (pending NARA approval).

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		
State, local, tribal gov't entities	X			
Public	X			
Private sector	X			
Foreign governments				

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Foreign entities				
Other (specify):	X			

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.)

ECRD will operate on JCON, a secure DOJ network. Entry to the system will be through secure login (which will only be given to OPA staff). Mandatory training will be required of all system users before ECRD goes live, and for any new users before they may gain access to the database. Finally, a thorough audit trail keeps track of everything a user does within ECRD

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: "Important Notice to Applicants," which is available on OPA website preceding each application. Additionally, the pardon application contains an "Authorization for Release of Information" page, which informs the petitioner of what types of information we may obtain and how we may obtain the information. Petitioners must sign this authorization as part of their application.
	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: Petitioners have the option not to provide their SSN. Additionally, as

		outlined in "Important Notice to Applicants," petitioners need not apply if they don't want personal/identifying information to be used by OPA.
	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.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: Petitioners' permission is implicit in their submission of an application for presidential clemency. The application is considered consent to particular uses of information. Additionally, the pardon application contains an "Authorization for Release of Information" page, which informs the petitioner of what types of information we may obtain and how we may obtain the information. Petitioners must sign this authorization as part of their application.
	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not:

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.

"Important Notice to Applicants" was crafted for the sole purpose of fully informing an applicant of what information may be used/gathered in the processing of their petition for presidential clemency and explaining why this information is needed. It provides full disclosure to the petitioner of what the ultimate consequences of applying for presidential clemency might be. The notice informs the petitioner of the authority by which we obtain information. Finally, the notice informs the petitioner of to whom and under what circumstances we will release information regarding a clemency application. The purpose of this notice is to ensure petitioners fully understand the possible uses of their personal information by this office.

Section 6: Information Security

6.1 Indicate all that apply.

	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: A thorough audit trail is created based on anything a user accesses in ECRD.	
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Mandatory training for users; usernames/passwords necessary for access to ECRD.	
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: Certification and Accreditation is currently in progress.	
	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:	
	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
	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.

Though entry to ECRD is achieved through a web portal, access can only be gained by computers on the JCON network. Further, a person seeking access requires a valid username and password. Username/passwords are given only to OPA staff who have completed the mandatory training on how to handle sensitive information.

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.)

	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:
X	Yes, and a system of records notice is in development. A current SORN is in existence. In addition, a revised SORN has been prepared and is expected to be published in the near future, under the title " Executive Clemency Files/Executive Clemency Records Database."
	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 on US Citizens as well as lawfully admitted resident aliens will be retrieved, as with all petitioners, by looking up any uniquely identifying personal information. This includes but is not limited to: name, BOP register number, FBI number, and SSN (see answer to question 1(e), above).