Office of the Pardon Attorney

Privacy Impact Assessment
for the
Electronic Clemency Records Database

Issued by:
William Taylor II
Executive Officer/SCOP

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: October 30, 2019

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The Office of the Pardon Attorney (PARDON) receives and reviews petitions for all forms of executive clemency, including pardon, commutation (reduction) of sentence, remission of fine or restitution, and reprieve. It also initiates the necessary investigations of clemency requests, and prepares the report and recommendation of the Attorney General, or his designee, to the President on each clemency request. This office maintains a clemency case file for each individual who has applied for or has been granted or denied clemency. The office also acts as liaison with the public for correspondence and informational inquiries about the clemency process or particular clemency issues, and maintains correspondence files relating to such inquiries. The office serves as the repository of historical records pertaining to the granting of clemency, and maintains copies of the warrants and proclamations of clemency granted by the President.

PARDON utilizes the Electronic Clemency Records Database (ECRD)[1] to serve as the primary record-keeping repository for presidential clemency applications and clemency related correspondence and records. All documents pertaining to a clemency petition ultimately used by the Department and the President to make a final disposition in each case are housed in ECRD. Information in identifiable form, such as name, social security number (SSN), and other government issued identifiers is collected, maintained, or disseminated by ECRD of individuals who are the subject of the application.

Section 2: Purpose and Use of the Information Technology

2.1 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. Executive clemency case files and records contained within ECRD are maintained by the Attorney General, or his designee, to facilitate and document the functions of the Attorney General, or his designee, in receiving, investigating, and evaluating requests for executive clemency; preparing the necessary reports and recommendations from the DOJ to the President in clemency matters; serving as a liaison with clemency applicants and the public on clemency matters; and advising the President on the historical exercise of the clemency power. The system's use of computerized records facilitates an increased level of efficiency and automation with regard to the maintenance and use of information contained therein.

Additionally, at the request of the Office of the Deputy Attorney General, PARDON may pull its own credit reports/summaries, as well as criminal rap sheets. Previously, PARDON had to make individual requests to the FBI to pull both documents. However, PARDON now has the ability to pull criminal rap sheets and outstanding warrant information directly from FBI's Criminal Justice Information Systems (CJIS). PARDON is also working with the Department's Office of General Counsel to obtain access to pull credit reports/summaries.

[1] DOJ/OPA-001, Executive Clemency Case Files/Executive Clemency Tracking System, 76 Fed. Reg. 57078 (Sept. 15, 2011), https://www.govinfo.gov/content/pkg/FR-2011-09-15/pdf/2011-23599.pdf

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/References
X	Statute	28 U.S.C. §§ 533, 534 (1966); the Uniform Federal Crime Reporting Act of 1988 (Pub. L. 100-690); and 44 U.S.C. § 3101 (1968).
X	Executive Order	Exec. Order No. 11878 (1975).
X	Federal Regulation	28 C.F.R. §§ 0.35-0.36 (1983); 28 C.F.R. § 0.85 (1969); and 28 C.F.R. §§ 1.1-1.11 (1993).
	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	U.S. Const. art. II, § 2.

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Name	X	C, D	*Name of members of the public (US and non-USPERs)*
Date of birth or age	X	C, D	*DOB of members of the public (US and non-USPERs)*
Place of birth	X	C, D	*POB of members of the public (US and non-USPERs)*
Gender	X	C, D	*Gender of members of the public (US and non-USPERs)*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Race, ethnicity or citizenship	X	C, D	*Race and Citizenship of members of the public (US and non-USPERs)*
Credit Summary	X	C,D	*Credit Report Summaries of the public (US and non-USPERs)*
Criminal Rap Sheet	X	C,D	*FBI criminal rap sheet of clemency petitioners ((US and non-USPERs)*
BOP Register Number	X	C,D	*BOP Register Number of clemency petitioners ((US and non-USPERs)*
Religion	X	C, D	*Religion of members of the public (US and non-USPERs)*
Social Security Number (SSN)	X	C, D	*Full SSN of members of the public (US and non-USPERs)*
Tax Identification Number (TIN)	X	C, D	*TIN of members of the public (US and non-USPERs)*
Driver's license	X	C, D	*Driver's license of members of the public (US and non-USPERs)*
Alien registration number	X	C, D	*Alien number of members of the public (non-USPERs)*
Passport number	X	C, D	*Passport of members of the public (US and non-USPERs)*
Mother's maiden name	X	C, D	*Mother's maiden name of members of the public (US and non-USPERs)*
Vehicle identifiers	X	C, D	*Vehicle information of members of the public (US and non-USPERs)*
Personal mailing address	X	C, D	*postal addresses of members of the public (US and non-USPERs)*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Personal e-mail address	X	C, D	*Personal email addresses of members of the public (US and non-USPERs)*
Personal phone number	X	C, D	*Personal phone number of members of the public (US and non-USPERs)*
Medical records number	X	C, D	*Medical record number of members of the public (US and non-USPERs)*
Medical notes or other medical or health information	X	C, D	*Medical, psychological, and health records of members of the public (US and non-USPERs)*
Financial account information	X	C, D	*Financial records of members of the public (US and non-USPERs)*
Applicant information	X	C, D	*Applicant information of members of the public (US and non-USPERs)*
Education records	X	C, D	*Educational records of members of the public (US and non-USPERs)*
Military status or other information	X	C, D	*Military status and information of members of the public (US and non-USPERs)*
Employment status, history, or similar information	X	C, D	*Employment status and history of members of the public (US and non-USPERs)*
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C, D	*Performance ratings of members of the public (US and non-USPERs)*
Certificates	X	C, D	*Educational and licensing certificates of members of the public (US and non-USPERs)*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Legal documents	X	C, D	*Legal records of members of the public (US and non-USPERs)*
Foreign activities	X	C, D	*Foreign activity records of members of the public (US and non-USPERs)*
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C, D	*Criminal charges, arrests, rap sheets and history of members of the public (US and non-USPERs)*
Juvenile criminal records information	X	C, D	*Juvenile criminal records of members of the public (US and non-USPERs)*
Civil law enforcement information, e.g., allegations of civil law violations	X	C, D	*Civil enforcement and law violations of members of the public (US and non-USPERs)*
Grand jury information	X	C, D	*GJ material of members of the public (US and non-USPERs)*
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C, D	*Victim/Witness information and records of members of the public (US and non-USPERs)*
Procurement/contracting records	X	C, D	*Procurement and contracting records of members of the public (US and non-USPERs)*
Proprietary or business information	X	C, D	*Proprietary business information of members of the public (US and non-USPERs)*
Biometric data:			
- **Photographs or photographic identifiers**	X	C, D	*Photographs of members of the public (US and non-USPERs)*
- **Video containing biometric data**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Fingerprints**	X	C, D	*Fingerprints of members of the public (US and non-USPERs)*
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	C, D	Scars, marks, tattoos *of members of the public (US and non-USPERs)*
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**	X	C, D	*Evaluations and recommendations will be recorded in and/or attached to workflows.*
System admin/audit data:			
- **User ID**	X	A	*DOJ Employee and contractors*
- **User passwords/codes**	X	A	*DOJ Employee and contractors*
- **IP address**	X	A	*DOJ Employee and contractors*
- **Date/time of access**	X	A	*DOJ Employee and contractors*
- **Queries run**	X	A	*DOJ Employee and contractors*
- **Content of files accessed/reviewed**	X	A	*DOJ Employee and contractors*
- **Contents of files**	X	A	*DOJ Employee and contractors*

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

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

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Other Federal entities; U.S. District Courts and U.S. Probation Office					

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

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	PARDON shares case information within the component by sending electronic notices from within the ECRD alerting an employee that they need to use their unique login credentials to access the system.
DOJ Components	X			PARDON shares information with other DOJ Components/Stakeholders of the clemency process by initiating an email be sent directly from the ECRD to the employees DOJ email account to include relevant attached records for review and consideration.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal entities	X			Pursuant to 28 C.F.R. § 1.5, petitions, reports, memoranda, and communications submitted or furnished in connection with the consideration of a petition for executive clemency generally shall be available only to the officials concerned with the consideration of the petition. However, they may be made available for inspection; in whole or in part, when in the judgment of the Attorney General, Deputy Attorney General, or Pardon Attorney, their disclosure is required by law or the ends of justice.
State, local, tribal gov't entities	X			Pursuant to 28 C.F.R. § 1.5, petitions, reports, memoranda, and communications submitted or furnished in connection with the consideration of a petition for executive clemency generally shall be available only to the officials concerned with the consideration of the petition. However, they may be made available for inspection; in whole or in part, when in the judgment of the Attorney General, Deputy Attorney General, or Pardon Attorney, their disclosure is required by law or the ends of justice.
Public		X		According to law and policy, PARDON is required to publicly and proactively disclose certain information on PARDON's public-facing website as required by the Freedom of Information Act (FOIA).

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Pursuant to 28 C.F.R. § 1.5, petitions, reports, memoranda, and communications submitted or furnished in connection with the consideration of a petition for executive clemency generally shall be available only to the officials concerned with the consideration of the petition. However, they may be made available for inspection; in whole or in part, when in the judgment of the Attorney General, Deputy Attorney General, or Pardon Attorney, their disclosure is required by law or the ends of justice.
Private sector	X	X		FOIA requires PARDON to disclose certain records to the public upon request if they do not fall within the narrow 11 exemptions. 5 U.S.C. § 552
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

Pardon does not submit data from the ECRD for "Open Data" purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

All petitioners are informed of DOJ's disclosure responsibilities in the acknowledgement of the receipt of a new petition. Information about disclosure policies is also publicly available on PARDON's Frequently Asked Questions page at https://www.justice.gov/pardon/frequently-asked-questions.

Forms related to commutations and pardons include Privacy Act (e)(3) statements. The Privacy Statement for Commutation of Sentence cases is publicly displayed on the Department's website and available for download at https://www.justice.gov/pardon/file/960571/download. The Privacy Statement for Pardon after Completion of Sentence cases is also publicly displayed on the Department's website and available for download at https://www.justice.gov/file/1113616/download.

The PARDON system of records notice (SORN), JUSTICE/OPA-001, *Executive Clemency Case Files/Executive Clemency Tracking System*, also provides notice to the public. The SORN is available for review at https://www.justice.gov/opcl/doj-systems-records#OPA.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Most of the non-law enforcement sensitive information provided in connection with an executive clemency case is provided directly by, or on behalf of the subject of the clemency request. Information is also received from petitioners' legal counsel or family members, at the request of the petitioner. With regard to dissemination, explicit permission is required from the subject using the Department's FORM DOJ-360 ***Authorization to Release Information to Another Person***. A Certification of Identity form is available online at http://www.justice.gov/oip/doj-reference-guide-attachment-d-copies-forms. *See* 28 C.F.R. § 16.3(a)(3).

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Records maintained by PARDON in the ECRD are exempt from the access and amendment provisions of the Privacy Act. *See 28 C.F.R. § 16.79*. However, access may be available through a Freedom of Information Act request with a signed Certification of Identity form available at http://www.justice.gov/oip/doj-reference-guide-attachment-d-copies-forms. *See* 28 C.F.R. § 16.3(a)(3).

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO): PARDON's ATO expires on October 12, 2020** **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** The ATO for PARDON's ECRD expires on October 12, 2020.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** JMD-OCIO manages our system and server and they perform routing monitoring, testing and evaluation of data.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** JMD-OCIO manages our system and server but the Pardon Attorney, Executive Officer and support staff review monthly reports to audit the data within the ECRD and use such audits to provide reports to the Deputy Attorney General, Office of White House Counsel, and post aggregated data to the clemency statistics page on the Department's website at https://www.justice.gov/pardon/clemency-statistics each month.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** In addition to the mandatory onboarding training, PARDON provides hands-on, individualized, and role-based training to each new employee, intern and contractor. Rights within the system are role based and approved by a PARDON management team member after a system request form and updated rules of behavior form have been completed and approved.

6.2 ***Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible***

unauthorized access?

PARDON's ECRD is not accessible outside of a DOJ firewall/network and not accessible within DOJ without a controlled, role-based user profile. Internal system access controls are utilized to reduce the risk of unauthorized disclosure by placing limitations on certain roles within the system (i.e. certain role-based users are not authorized to trigger the system to send outgoing correspondence without system approval of their direct supervisor).

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

All records within ECRD are maintained while a clemency petition is pending. When a case is closed, all records pertaining to the case file are maintained in ECRD for fifteen to twenty-five years following the closing date. Once the retention period has lapsed, all records pertaining to the closed case are copied and sent to National Archives and Records Administration (NARA). Once NARA becomes the legal custodian of the records, the records within ECRD are destroyed. This change occurs in accordance with Records Disposition Authority DA–204–2011–0001 or successor Records Disposition Authority.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

Information on petitioners, including U.S. Citizens and lawfully admitted resident aliens, may be retrieved by the following personally identifiable information: petitioner's name, Bureau of Prisons register number, FBI number, and SSN.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

DOJ/OPA-001, *Executive Clemency Case Files/Executive Clemency Tracking System*, 76 Fed. Reg. 57078 (Sept. 15, 2011), https://www.govinfo.gov/content/pkg/FR-2011-09-15/pdf/2011-23599.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

a. Potential Threats Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish the Department's official duties is always a potential threat to privacy. PARDON only collects and receives information on individuals that allows the Deputy Attorney General to approve the Department's letters of advice, and informs the President's decision to approve or deny petitions for executive clemency. For example, PARDON collects information on individuals' home address and contact information, in order to communicate with petitioners who are not incarcerated directly, results of fingerprints are included in criminal rap sheets, and Petitioners often submit photographs of themselves and their family as evidence of an inmate's support system. While a great deal of information is collected about individuals, the vast majority of information is supplied by the clemency subject themselves. When the subject of clemency submits information, there is an understanding that PARDON will only collect and disclose information and records as necessary to ascertain and report on the totality of their circumstances for relief consideration. Petitioners are also advised that if they choose not to respond or refuse to provide requested information and/or documentation that would be helpful in analyzing their clemency request, it is possible that the case will be administratively closed without presidential action and without prejudice.

Additionally, petitions, reports, memoranda, and communications submitted or furnished in connection with the consideration of a petition for executive clemency generally shall only be available to the officials concerned with the consideration of the petition. However, they may be made available for inspection; in whole or in part, when in the judgment of the Attorney General, Deputy Attorney General, or Pardon Attorney, their disclosure is required by law or the ends of justice.

b. Potential Threats Related to Use of the Information

Potential threats to privacy as a result of the Department's use of the information in the ECRD System include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access or improper disposal of information, and unauthorized disclosure of the information.

PARDON mitigates these risks by only granting access internally to PARDON staff who have obtained the requisite clearance and the proper request form and/or identity validation has occurred. Access to the system is role-based and users are only authorized to access information that they need to know to perform their job duties. Mandatory training is required of all system users before they may gain access to the database. Information and records with PII are encrypted by the sender for additional security when transmitting information to non-DOJ government entities. Finally, audits are conducted at regular intervals to ensure that there is no improper use by users. Auditing such data and making users aware of the detailed audit trail on every action in the system limits privacy and security risks. For a list and description of additional security controls that have been put into place to safeguard against these and other risks, please see the responses to questions 6.1 through 6.3.

c. Potential Threats Related to Dissemination

The Pardon Attorney may disclose the contents of executive clemency files when the disclosure is required by law or the ends of justice. On the other hand, non-public documents that may be compiled in the course of processing a clemency application, such as the petition and supporting documents, the

presentence investigation report, the results of any federal background investigation, and the recommendation of the Department of Justice, are not generally available under the Freedom of Information and Privacy Acts. However, the President and his immediate staff are not subject to the constraints of the Freedom of Information and Privacy Acts. Accordingly, while clemency-related documents in the possession of the White House traditionally have not been made public, they may be legally disclosed at the discretion of the President. In addition, clemency-related documents retained by the White House at the end of a presidential administration will become part of the President's official library, where they become subject to the disclosure provisions of the Presidential Records Act.

Also, data files regularly, proactively released through the FOIA via PARDON's public website, for example through the "Lookup Function," are done so in compliance with applicable law and policy obligations. The Office of the Pardon Attorney is obliged to release existing lists of the names of persons who have been denied executive clemency by the President to anyone who requests such records pursuant to the Freedom of Information Act. Given the frequency of such requests, the Pardon Attorney has started to proactively disclose the names of persons who have been denied executive clemency by the President on our website. PARDON also proactively discloses the names of those who have been granted clemency and provides a downloadable PDF file of the President's clemency warrant for more recent administrations.

While unauthorized disclosures are a possibility due to user error, PARDON mitigates risks by being selective about user access, providing extensive system training, requiring users to be aware of and acknowledge understanding of the Department's Rules of Behavior on sensitive systems, enforcing strict system locks, having daily interaction and coordination with the user community and only providing user access to outside offices like the Office of the Deputy Attorney General, as needed. Security measures that are in place to safeguard sharing of information include: IT monitoring tools; firewalls; intruder detection and data loss prevention mechanisms; and audit logs.