Criminal Division

Privacy Impact Assessment
for the
Human Rights Violation (HRV) – United States Attorney's Office (USAO) Intake System (HUIS)

Issued by:
Jennifer A.H. Hodge
Criminal Division, Senior Component Official for Privacy

Approved by: Michelle Ramsden
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 2, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The United States Department of Justice (Department or DOJ), Criminal Division (Division), Human Rights and Special Prosecutions Section (HRSP) leads the Department's efforts to deny safe haven in the United States to human rights violators (violators). HRSP investigates and prosecutes violators for genocide, torture, war crimes, recruitment or use of child soldiers, female genital mutilation, and for immigration and naturalization fraud arising out of efforts to hide their involvement in such crimes.

Due to the specialized nature of these type of investigations and the unique jurisdictional questions that arise from crimes committed in foreign countries, the Department requires HRSP to act as the ombudsman for these matters[1] from the point of inception, in order to ensure their optimal handling. Because these matters are not sufficiently mature to be recorded in the Division's case tracking system, HRSP has been tracking these internally through a manual process for many years. HRSP seeks to improve this tracking process by standing up the Human Rights Violation (HRV) – United States Attorney's Office (USAO) Intake System (HUIS). The Division conducted this Privacy Impact Assessment to assess and mitigate the risks to the Personally Identifiable Information (PII) collected in HUIS, which includes but is not limited to identifying information of subjects of matters, including citizenship or immigration status, and professional contact information for the potential eventual investigative and prosecutorial personnel.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

HRSP's work is part of a coordinated, interagency effort. HRSP's attorneys and historians work closely with Department of Homeland Security's, Homeland Security Investigations, the Federal Bureau of Investigation (FBI), the Department of State, the Department of Defense, and other national and international agencies to pursue accountability for human rights violators in a variety of ways.

Due to the specialized nature of the type of investigations arising from referrals and the unique evidential and jurisdictional questions that arise from crimes committed in foreign countries, the Department requires that Federal prosecutors notify, consult, or receive approval from HRSP upon opening matters involving human rights violators, as well as before performing

[1] A matter is the predecessor to a formal investigation or prosecution. From the time information is received that indicates a criminal offense may have occurred, to the point where enough information is gathered to confirm a formal investigation is warranted and may result in a prosecution, it is referred to as a matter.

specific investigative or prosecutorial actions.[2] Also, HRSP will often partner with USAOs on human rights related cases or serve as an advisor on some matters. Finally, because many of these matters overlap with national security offenses, DOJ mandates the consultation, notification, and prior approval of certain investigations with the Counterterrorism Section of the Department's National Security Division (NSD).[3]

Because these matters are often not sufficiently mature to be recorded in the Division's case tracking system, HRSP has been tracking these internally through a manual process for many years. HRSP seeks to improve this tracking process through the implementation of a formal database in response to the Deputy Attorney General's call to improve coordination with USAO personnel in the May 26, 2021, memorandum titled Comprehensive Strategy for Reducing Violent Crime. In this, HRSP hopes to standardize reporting, improve the quality of information sharing with its law enforcement and prosecutorial partners, improve historical documentation quality, and develop analytical capabilities for these referrals, notifications, consultations, approvals, investigations, and prosecutions by standing up HUIS under the Division's Custom Database Application System (CDAS). HUIS will be an internal-use-only database that documents each of the matters mentioned or referred to HRSP, along with the nature of the mention or referral, subject(s) of matters, geographic location of the subject(s), mentioning or referring entity, and a chronology of the decisions relating to the matter.

HUIS collects a narrowly defined scope of information, designed to document, and track matters which are being mentioned or referred to HRSP but are not yet ripe for entry into the Division's case tracking system. The information collected will typically include:

- Reporting date,
- Identifying information for the potential target, including relevant citizenship or immigration information,
- Assistant United States Attorney (AUSA) or law enforcement official reporting the information and their contact information,
- Law enforcement agency and personnel involved in the referral with their contact information,
- Country and location of the alleged human rights violations,
- Date of the alleged human rights violations,
- Description of the alleged offense(s),
- Chronology and description of communications regarding the matter,
- Name of the HRSP employee contacted,
- NSD referral date and contact (when applicable),
- Whether the case is a joint case with HRSP, and
- Whether further consultation will be necessary.

Should a matter mature to the point where it is believed to merit investigation or prosecution, HRSP or the other involved investigating and prosecuting entities will create an official case file[4] to contain the investigative and prosecutorial documents. Information from HUIS can be

---

[2] Justice Manual 9-2.139, and 9-142.000.
[3] Justice Manual 9-2.139.
[4] Should a referral mature into an investigation the source USAO will maintain the official case file in their "Case

reported to state, local, other Federal, tribal on foreign law enforcement or prosecutorial authorities should the substance of the matter be deemed relevant to them. Reports can be generated for dissemination to HRSP or other stakeholders for operational, performance or analytical needs. Reports may contain the PII of the subjects of matters.

Access is limited to HRSP personnel and those Criminal Division Information Technology (IT) personnel responsible for repairs, upgrades or help functions. HRSP attorneys and historians, paralegal specialists, and an internal administrator will be able to input data, view records, and run reports. A designated administrator will be able to manage account access. On a case-by-case basis, reports may be provided to law enforcement or prosecutorial partners with a verified need. In specific instances where HRSP is partnering with foreign authorities, reports may be provided to those authorities after management review and approval.

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/Reference
☒ Statute	5 U.S.C. § 301; 8 U.S.C. §§ 1451, 1227(a)(4)(D), 237(a)(4)(D); 1182(a)(3)(E), 212(a)(3)(E); 18 U.S.C. §§ 116, 1015, 1091-1093, 1425, 1546, 2340, 2340A, 2340B, 2441, 2442; 28 U.S.C. §§ 516, 510, 519; 44 U.S.C. § 3101
☐ Executive Order	
☒ Federal Regulation	28 C.F.R. part 0, subpart K—Criminal Division
☐ Memorandum of	
☒ Justice Manual[5]	Title 9: Criminal 9-2.139, 9-142.000, 9-90.020
☒ Other (summarize and provide copy of relevant portion)	Human Rights Enforcement Act of 2009; May 26, 2021, Memorandum from The Deputy Attorney General: Comprehensive Strategy for Reducing Violent Crime

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).

Management Enterprise System," since all HRSP HRV cases are litigated in concert with a USAO, and the USAO maintains the official case file. HRSP will provide relevant information from this system to the USAO for incorporation into the official case file. At the conclusion of an investigation or prosecution, the case paralegals will conduct a comparison and de-duplication of the case files, to ensure the USAO possesses a complete version of the case file. Information in HRSP's system will be deleted when no longer needed.

[5] https://www.justice.gov/jm/justice-manual.

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
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C & D	HRSP POC, AUSA POC, law enforcement POC, Subjects of matters and associates
Date of birth or age	X	C & D	Subjects of matters
Place of birth	X	C & D	Subjects of matters; although not specifically solicited, this may appear in the description of the offense.
Gender	X	C & D	Subjects of matters and associates; although not specifically solicited, this may appear in the description of the offense.
Race, ethnicity, or citizenship	X	C & D	Subjects of matters and associates; citizenship information is specifically solicited. Race or ethnicity is not specifically solicited but may appear in the description of the offense.
Religion	X	C & D	Subjects of matters; although not specifically solicited, this may appear in the description of the offense.
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C & D	Subjects of matters
Passport number	X	C & D	Subjects of matters
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Professional e-mail address	X	A & B	AUSA POC, law enforcement POC
Professional phone number			
Social Media Identifiers			
Medical records number			

(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
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information	X	C & D	Subjects of matters and associates; although not specifically solicited, this may appear in the description of the offense.
Employment status, history, or similar information	X	C & D	Subjects of matters and associates
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	x	C & D	Subjects of matters and associates; to the extent this information is relevant to the referral
Web uniform resource locator(s)			
Foreign activities	X	C & D	Subjects of matters and associates; to the extent this information is relevant to the referral
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C & D	Subjects of matters and associates; to the extent this information is relevant to the referral
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C & D	Subjects of matters and associates; to the extent this information is relevant to the referral
Whistleblower, e.g., tip, complaint, or referral	X	C & D	To the extent this information is relevant to the referral
Grand jury information	X	C & D	Subjects of matters and associates; to the extent this information is relevant to the referral
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C & D	To the extent this information is relevant to the referral
Procurement/contracting records			
Proprietary or business 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
Location information, including continuous or intermittent location tracking capabilities	X	C & D	Subject of matters and associates, to include physical location at specific times to the extent this information is relevant to the referral.
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	This system captured audit data as mandated in National Institute of Standards and Technology (NIST) special publication (SP) 800-53, Revision 4.[6]
- **User ID**	X	A	
- **User passwords/codes**			
- **IP address**	X	A	
- **Date/time of access**			
- **Queries run**			
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):	X	C & D	Information in this chart is anticipated information that may be provided in the narrative description of the matter. However, given the varied nature of the Division's work, the information placed into HUIS could include any type of lawfully obtained, unclassified information reasonably necessary for or relevant to a referral.

[6] *See* https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22.

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

Directly from individual about whom the information pertains		
☒ In person	☒ Hard copy: mail/fax	☒ Online
☒ Telephone	☒ Email	
☐ Other (specify):		
☒ Explanation:	Contact information for the law enforcement or prosecutorial contacts may be collected directly from the individual about who it pertains.	

Government sources		
☒ Within the Component	☒ Other DOJ components	☐ Other federal entities
☒ State, local, tribal	☒ Foreign	
☐ Other (specify):		
☒ Explanation:	Contact information for the law enforcement or prosecutorial contacts and information about the subject(s) of the matter will be collected directly from government sources.	

Non-government sources		
☐ Members of the public	☐ Public media, internet	☐ Private sector
☐ Commercial data brokers		
☐ 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	☒	☐	☒	Within HRSP access is limited to the internal system administrator and attorney, historian or paralegal with a need-to-know can directly access the system. Within-Component sharing for all other personnel is the same as described below.

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.**
DOJ Components	☒	☐	☐	Information contained in this system is tailored to include the initial referral or allegation of a matter and how that matter is handled from a decisional standpoint. It is not considered an investigative file or treated as evidence. Therefore, the Department does not anticipate significant sharing of HUIS data. However, should sharing the information be deemed appropriate to further the Department's mission to identify and prosecute international human rights violators, or to deconflict investigative efforts, it could be shared with both U.S.-based or international law enforcement, prosecutorial or judiciary personnel on a case-specific basis, in accordance with the Privacy Act and any relevant Systems of Records Notices.
Federal entities	☒	☐	☐	
State, local, tribal gov't entities	☒	☐	☐	
Public	☐	☐	☐	
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	☒	☐	☐	
Private sector	☐	☐	☐	
Foreign governments	☒	☐	☐	
Foreign entities	☒	☐	☐	
Other (specify):	☒	☐	☐	Statistical information may be contained within reports to officials outside DOJ (e.g., Congress) concerning Division caseload, activities, performance, and resource requests.

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.

This information will not be released to the public for "Open Data" purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals or the public providing information about the collection, use, sharing or other processing of covered 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.

The public is provided with general notice of the existence of referrals, allegations, and matters through Division SORN CRM-001, Central Criminal Division Index File and Associated Records last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007) and amended at 82 Fed. Reg. 24155 (May 25, 2017).

The public is provided with general notice of Department of Justice computer systems through Department JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access, last published in full at 86 Fed. Reg. 37188 (July 14, 2021).

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.

The public is provided with general notice of the existence of case files through the System of Records Notice, Central Criminal Division Index File and Associated Records, JUSTICE/CRM-001. Generally, individuals are not given the opportunity to voluntarily participate in the collection, use or dissemination of their information in the system, or to consent to specific uses, as it may jeopardize ensuing law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation.

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.

Information in this system is exempt from the access, amendment, correction, and notification procedures of the Privacy Act.[7] Accordingly, individuals who are the subject of the records generally will not be provided with Privacy Act access or amendment capabilities to the records in HUIS, as doing so may jeopardize ensuing law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation.

Although exemptions may apply, individuals may make access requests for information maintained in this system via the Freedom of Information Act (FOIA).[8] Such requests will be processed according to the provisions of the FOIA.

Matters documented in this system may mature into investigations and prosecutions, in which case the information contained in the underlying referral will be compiled into the relevant investigatory and prosecutorial case files.

---

[7] As relates to JUSTICE/CRM-001, exemptions are claimed pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). *See* 28 C.F.R. § 16.91. As relates to JUSTICE/DOJ-002, exemptions are claimed pursuant to 5 U.S.C. 552a (k)(1) and (k)(2). *See* 86 FR 61687.

[8] *See* https://www.justice.gov/criminal/crm-freedom-information-act.

The Department anticipates that any sharing of the underlying information, including sharing during pre-trial or trial, will occur from those case files and will be handled in accordance with the relevant SORNs.

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).

☒	**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):** HUIS will be a subsystem of the Division's Custom Database Applications System (CDAS) for which the ATO expiration date is October 10, 2025. **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:** All ATO process and risk assessment materials, including the existence of POAMs resulting from those processes, are recorded in the Justice Management Division (JMD) Joint Cybersecurity Assessment and Management System (JCAM) records for the CDAS system. This information is normally considered Information System Vulnerability Information and is controlled by the relevant Information System Security Officer.
☐	**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:**
☒	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** The highest risk information contained in HUIS is related to investigative referrals and is considered a moderate risk in accordance with FIPS 199 and includes appropriate security controls for this categorization, and the sensitivity of the information.
☒	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** CDAS undergoes continuous assessments, penetration tests, and vulnerability scans, and is monitored through the Division IT Security Continuous Monitoring Program.

	The Division performs vulnerability and configuration management scanning using both tools provided by the DOJ Office of the Chief Information Officer and provided by Division IT. Continuous monitoring includes the security assessment process, and a manual review audit occurs at regular intervals, to the extent required by the National Institute of Standards and Technology (NIST) special publication (SP) 800-53, Revision 4.[9]
☒	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The Division collects logs according to the standards in the DOJ Cybersecurity Standards, which include Operating System, Web, Database and Application logs for every FISMA-applicable system. Logs are correlated into appropriate DOJ information systems managed by JMD. Access to these logs is provided to the Justice Security Operations Center, who provided security analysis and log monitoring for unusual activity to the extent required by NIST SP 800-53, Rev. 4. Information Owners and Stewards that identify additional audit review requirements per the NIST control selections in their System Security Plan and further defined by entries in a Continuous Monitoring Implementation Plan (Division Template), may have reports designed to monitor for unusual activity. These reports would be reviewed on the as described above, or in the event of suspicious activity as determined by the HRSP Supervisors and IT personnel.
☒	**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**.
☒	**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:** One-on-one training, specific to this system, is conducted for authorized users by the HRSP internal system administrator.

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?

All Division systems implement technical security to reduce the risk of compromise to PII information. Specifically, certain access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure, including but not limited to the following:

- HUIS has a security categorization of FISMA Moderate and has selected

[9] *See* https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22.

appropriate security controls for this categorization, and the sensitivity of the information. The Division will not input any information that would be categorized as "High" under NIST FIPS Publication 199, or NIST SP 800-60, Volume II, into this system without the approval of appropriate privacy and security personnel, to ensure adequate controls are applied to protect such information.

- The system is accessible by DOJ employees and contractors only and utilizes tiered, role-based access commensurate with the end-user's official need to access information. Physical access to system servers is controlled through site-specific controls and agreements. Access to this system is granted on a need-to-know basis, based on the principle of least information necessary to perform the job, and is individually verified through the employees Personal Identity Verification (PIV) card.
- The system is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.
- All users must complete annual Cyber Security and Awareness Training (CSAT) training, as well as read and agree to comply with DOJ Information Technology and Privacy Rules of Behavior. HUIS system administrators must complete additional professional training, which includes security training.
- Audit logging is configured, and logs are maintained to help ensure compliance with tiered access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access.

Overall, HUIS's defense-in-depth measures are designed to mitigate the likelihood of security breaches and allow the Department time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

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.)

Disposition of records within HUIS will conform to processes and procedures established by the Division Records Management Section (RMS) for the disposition of softcopy records. These records will be maintained in accordance with Records Schedule DAA-0060-2021-0001.

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. ☒ Yes.

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:***

SORN JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007) and amended at 82 Fed. Reg. 24155 (May 25, 2017).

SORN JUSTICE/DOJ-002, DOJ Computer Systems Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 14, 2021).

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?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

Privacy Risk: Unauthorized access or misuse of information
Mitigation: CRM employs a robust physical security system to protect its servers and access terminals, including secure worksites, armed guards, cameras, and access restricted office suites. HUIS also implements access monitoring and privacy and records controls standardized by the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems, as defined in NIST Special Publication 800-53.

Employee access to this system is limited based on a need-to-know and further limited by restrictions which limit users to the minimum access needed. Once those criteria are met and management approval is received, access is granted. This system utilizes a user's PIV card and pin number for authentication. It also has been evaluated and authorized to operate according to the risk management framework required by FISMA.

An audit log is maintained of all user logins and actions. Notification of the monitoring is presented clearly when logging into the system. Additionally, DOJ employees and contractors must complete annual training regarding handling of PII as part of the Department's CSAT, as well as read and agree to comply with DOJ Information Technology

and Privacy Rules of Behavior. This occurs during their orientation upon entering into service with DOJ and annually thereafter. Additionally, the Section provides one-on-one training for employees granted access to HUIS. The Division maintains an Account Management Guide and Configuration Management Guide for HUIS.

The IT system assessment is documented in the JMD JCAM assessment tool and maintained as part of the ongoing authorization and assessment plan. All security controls are documented in the System Security and Privacy Plan recorded in the IT system. There is no outside access to this system; administrator access is restricted to the few DOJ employees and contractors who administer the program.

Privacy Risk: Name association with the database
Mitigation: As in most cases where a record associates a person with a potential criminal investigation, the mere presence of a name in the system can generate the assumption of involvement with criminal activity or other damage to their reputation. In the case of this system, the alleged offenses underlying referrals are some of the most egregious. For this reason, this is a closed system with no access outside of HRSP and limited internal access to only those senior, trained employees with a need to know. There is no automated dissemination of information from this system outside of the HRSP. Any dissemination must be done pursuant to proper authority and management review. Information obtained from this system is considered law enforcement sensitive and the screens within it are so marked. Additionally, de-identification of management reporting is practiced in all instances possible.

Privacy Risk: Erroneous or inaccurate information, misidentification of a subject
Mitigation: Obtaining of complete and accurate information is complicated by the preliminary pre-investigation stage of information collections in this system, and the peripheral circumstances in which human rights violations often occur; in foreign countries, in circumstances were records are either not available, destroyed, or otherwise obfuscated.

These risks are mitigated by strictly tailoring the data collection to its purpose: the tracking of initial decisions made regarding the handling of a matter (i.e., who might investigate, who might prosecute, might it be a joint investigation, does NSD need to be notified). For those reasons, this database captures the minimum identification information necessary to distinguish the matter for tracking purposes, but not for more expansive evidentiary purposes. This means a matter could be identified by a group of individuals, or a location of an event instead of a name, if that is the only information available. Although the subject identification information contained in this system is minimal, it must contain specific identity verification information such as an Alien Registration Number, passport number or date of birth, if known, to ensure accuracy. In this way, the HRSP advances the fair information practice principle of data minimization.

Additionally, the Division relies on the reporting entity to verify the accuracy of the information. Reporting entities include eventual investigative personnel, prosecutorial personnel, trained historians, or foreign governments with an interest in identifying and bringing human rights violators to justice. Their information may arise from a variety of sources such as witnesses, surviving victims, media reports, court documents, or domestic and foreign government documents. In the case of human rights abuses, the reporting

entities are specialized subject matter experts. Agencies involved in the investigations which may arise from referrals have created their own specialized human rights offices[10] to allow their employees to constantly hone their skill set, gain an acute awareness of potential pitfalls in information collection, and acquire the ability to differentiate between accurate or questionable information. Additionally, these reporting entities have a vested interest in handling of these matters in the most diligent and accurate manner possible to ensure the successful handling of these matters. Once received by HRSP, the information is reviewed and assessed by internal human rights specialist attorneys and historians for entry into this system or potential requests for clarification of the information. Thus, every effort is made to diligently review, verify, and correct information from these records.

Privacy Risk: Over-collection
Mitigation: In order to mitigate over-collection concerns, the Division considered the careful minimization of information collection in the design of HUIS. HUIS has a customized entry screen that solicits and attempts to minimize information collection through structured data fields to meet HRSP's specific needs. In HUIS, sensitive identifiers such as dates of birth, alien number, or passport information were considered and determined to be necessary for the accurate identification of the subjects of matters. Should HRSP discern a need to add additional data collection fields beyond those anticipated at the time of this PIA approval, HRSP must obtain approval from the CRM senior component official for privacy prior to obtaining IT support to make such change. Likewise, Division IT will consult with the Division Privacy Unit regarding the Privacy related implications of changing any data fields.

Professional contact information entered into the system for the eventual investigative and prosecutorial personnel are minimal and strictly necessary to support communications.

[10] Such as U.S. Immigration and Customs Enforcement's Human Rights Violators & War Crimes Center and its Office of the Principal Legal Advisor, Human Rights Violator Law Division; FBI, International Human Rights Unit; and U.S. Department of Defense U.S. Army, Criminal Investigations Division, Terrorism and Criminal Investigations Unit (TCIU).