Criminal Division

Privacy Impact Assessment
for the
Special Approvals System

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

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

Date approved: [June 14, 2023]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The United States Department of Justice (Department), Criminal Division (Division), Office of Enforcement Operations (OEO) conducts legal analysis to support recommendations for authorization, and consultations for the use of certain sensitive investigative techniques, prosecutorial tools, and special administrative measures (collectively "special techniques"). Due to their sensitivity, use of those special techniques by federal prosecutors, Department attorneys, or federal law enforcement may require prior consultation with the Division or explicit authorization by a senior Department official. The Division is in the process of designing a new database titled the Special Approvals System (SAS) to consolidate and streamline the request, review, tracking, approval, and record keeping process of these special techniques.

The Division conducted this Privacy Impact Assessment (PIA) to assess and mitigate the risks to the personally identifiable information (PII) collected in this system, much of which is Law Enforcement Sensitive (LES), and includes but is not limited to, individual names, specific descriptions of criminal allegations against individuals, and, in limited circumstances, other individual identifiers, such as dates of birth (DOBs), Federal Bureau of Investigation Numbers (FBI#s), and contact information.

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.

The Criminal Division develops, enforces, and supervises the application of all federal criminal laws, except those specifically assigned to other Divisions. The Criminal Division and the 93 U.S. Attorneys have the responsibility for overseeing criminal matters, as well as certain civil litigation. In the scope of these activities, Criminal Division attorneys investigate and prosecute many nationally significant cases. In addition to its direct litigation responsibilities, the Division formulates and implements criminal enforcement policy and provides advice and assistance on criminal matters. When certain law enforcement or investigatory techniques are likely to result in the release of sensitive information or the application of complex legal issues, an in-depth analysis must be performed to ensure the proposed course of action is prudent and legal. This analysis advises the relevant Department decision maker, who may be the Attorney General, Deputy Attorney General, Assistant Attorney General for the Criminal Division, Deputy Assistant Attorneys General for the Criminal Division, the Director of OEO, or their delegates.

OEO manages the review and approval processes for many of these special techniques. The U.S. Attorney's Offices (USAOs), litigating components of the Department, litigating sections of the Division, and federal law enforcement agencies submit applications to use the special techniques under OEO's purview. After reviewing the application and, when appropriate, conferring with the submitter, OEO attorneys typically prepare a recommendation memorandum, analyzing whether the proposed course of action complies with the relevant statutes, case law, regulations, and Departmental policies. The recommendation memorandum apprises the appropriate senior Departmental official of the relevant issues involved in the application and advises whether

authorization is warranted or whether the applicable consultation requirements have been satisfied. In most instances, the senior Department official signs a letter, which OEO prepares, informing the submitter of the decision on the request.

OEO coordinates requests to authorize the following special techniques, which will be tracked in SAS:

- Consultations or Authorizations to Apply for Warrants to Search the Premises or Property of Subject Attorneys[1]
- Issuance of Subpoenas to Attorneys for Information Relating to the Representation of Clients[2]
- Use of Classified Investigative Technologies
- Courtroom Closures
- Multi-District (Global) Plea Agreements[3]
- Nolo Contendere Pleas[4]
- Alford Pleas[5]
- Notices of Intent to Prosecute Attorneys
- Dual and Successive Prosecution Policy ("Petite Policy") Waivers[6]
- Special Grand Jury Certifications[7]
- Touhy Requests[8]
- Indictments for Unlawful Flight to Avoid Prosecutions[9]
- Approval to Compel Testimony (Witness Immunity)[10]
- Requests for Special Confinement Procedures (Special Administrative Measures)[11]
- "S"- Nonimmigrant Visas[12]
- Sensitive Consensual Monitoring[13]
- Re-subpoenaing a Previously Contumacious Witness before Successive Grand Juries[14]
- Confidential Disinterested Third-Party Search Warrants[15]
- Declining to Prosecute Failure to Register with the Selective Service System[16]
- Prosecution after a Compulsion Order (Previously Immunized Witness)[17]

---

[1] JM 9-13.420
[2] JM 9-13.410
[3] JM 9-27.641
[4] JM 9-16.000
[5] JM 9-16.015
[6] JM 9-2.031
[7] 18 U.S.C. § 3331
[8] 28 C.F.R. §16.21, et seq.
[9] 18 U.S.C. § 1073
[10] JM 9-23.130
[11] JM 9-24.000
[12] JM 9-72.100
[13] JM 9-7.301
[14] JM 9-11.160
[15] JM 9-19.000
[16] JM 9-79.400
[17] JM 9-23.400

- News Media Policy Consultations[18]
- Issuance of Subpoenas to a Member(s) of the News Media[19]
- Use Subpoenas, 2703(d) or 3123 Orders to Obtain the Communications Records or Business Records of a Member of the News Media[20]
- Application for warrants to search the premises, property, communications records, or business records of members of the news media[21]
- Requests for authorization to charge or arrest a member(s) of the news media[22]
- Requests for authorization to question members of the news media[23]
- Requests for Retrocession/Acquisition of Federal Jurisdiction[24] [25]
- Certain Requests for Non-Prosecution or Deferred Prosecution[26]
- Requests for Authorization to Exercise Law Enforcement Powers by Offices of the Inspector General[27]
- Utilization of Persons in Custody of BOP or USMS for Investigative Purposes, or as Targets of Investigative Activity[28]
- Electronic Surveillance[29]
- Closed Circuit Television Monitoring[30]
- Other unique special techniques which may develop, in which the Department believes may warrant special review in order to assure compliance with legal of Departmental regulations.

At the present time, these request authorizations are tracked in a variety of manners, including databases, spreadsheets, and manual/paper tracking. Those matters that merely require consultation with OEO are handled internally and routed from OEO staff to OEO managers and leadership via email. For matters that require authorization by senior Department leadership, the incoming applications, recommendation memoranda, and other relevant attachments are loaded into the Front Office Tracking System (FOTS) or the OEO Title III Request Tracking System, and the matter is routed to the appropriate Department official for further action. Notice of a final decision is then provided to OEO, which provides notice of that decision to the requester. SAS will combine all of these processes into one streamlined, paperless system.

Pursuant to statutory authorities, regulations, and Department policies, the Division has previously collected and preserved this information. As such, SAS does not constitute a new type or collection purpose. Instead, it provides an enhancement to the administration and efficiency

---

[18] JM 9-13.400
[19] *See supra* note 18.
[20] *See supra* note 18.
[21] *See supra* note 18.
[22] *See supra* note 18.
[23] *See supra* note 18.
[24] JM 9-20.220 *et seq.*
[25] 25 U.S.C. § 1323
[26] JM 9-27.640
[27] Attorney General's Memorandum dated June 29, 1984 re: Guidelines for Legislation Involving Federal Criminal Law Enforcement Authority; 5 U.S.C. App.. 3 § 1 *et seq.*;
[28] JM 9-21.050
[29] 18 U.S.C. § 2516; JM 9-7.000
[30] JM 9-7.200

of the approval processes.

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. § 1323; 5 U.S.C. § 3001; 8 U.S.C. § 1101(a)(15)(S), 1182, 1184(k), 1255(j); 18 U.S.C. § 1073, § 2510, *et seq.,* § 3331, § 3001 *et seq.,* § 6001-6005; 22 U.S.C. § 2708; 25 U.S.C. § 1323; 42 U.S.C §§ 2000aa *et seq*.; 50 U.S.C. App § 462; 5 U.S.C. App. 3 § 1 *et seq.*
☐ Executive Order	
☒ Federal Regulation	8 C.F.R. § 212.4; 28 C.F.R. part 0, subpart K—Criminal Division; 28 C.F.R. §§ 0.175, 16.21 *et seq.*, 50.9, 50.10 *et seq.*, 59.428, 501.3
☐ Memorandum of Understanding/agreement	
☒ Justice Manual[31]	Title 9: Criminal; JM 9-1.6.000 *et seq.*, 2.031, 2.032, 7.010-302, 11.160, 13.400, 13.410, 13.420, 16.001, 16.010, 16.015, 19.000, 19.210, 9.220-221, 19.240, 20.220; 21.050; 23.000 *et seq*., 24.000, 24.1009, 27.500, 27.640-641, 72.000, 79.400
☒ Other (summarize and provide copy of relevant portion)	Federal Rule of Criminal Procedure 11. Deputy Attorney General's Memorandum of January 31, 2002; Delegation of Signature Authority Memos completed as needed, upon changes of administration or senior level officials; Attorney General's Memorandum of June 29, 1984 re: Guidelines for Legislation Involving Federal Criminal Law Enforcement Authority.

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

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
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 and D	Request submitter and subject of request*
Date of birth or age	X	C and D	Required for limited request types such as witness immunities and S-visas*
Place of birth	X	C and D	Required for limited request types such as S-visas*
Gender	X	C and D	Required for limited request types such as S-visas*
Race, ethnicity or citizenship	X	C and D	Required for limited request types such as S-visas*
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C and D	Required for limited request types such as S-visas*
Passport number	X	C and D	Required for limited request types such as S-visas*
Mother's maiden name	X	C and D	May be included as unstructured information for limited request types*
Vehicle identifiers			
Personal mailing address	X	C and D	Required for limited request types such as those that involve search warrants for a physical address*

(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 and D	May be required for limited request types such as those involving electronic surveillance, search warrants or subpoenas*
Personal phone number	X	C and D	May be required for limited request types such as those involving electronic surveillance, search warrants or subpoenas*
Medical records number	X	C and D	May be included as unstructured information for limited request types*
Medical notes or other medical or health information			
Financial account information	X	C and D	May be included as unstructured information for limited request types*
Applicant information	X	C and D	May be included as unstructured information for limited request types*
Education records			
Military status or other information	X	C and D	May be included as unstructured information for limited request types*
Employment status, history, or similar information	X	C and D	May be included as unstructured information for limited request types *
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents	X	C and D	Supporting documents in the form of unstructured data such as subpoenas, search warrants or affidavits may be included with requests*
Device identifiers, e.g., mobile devices	X	C and D	May be required for limited request types such as those involving electronic surveillance, search warrants or subpoenas*
Web uniform resource locator(s)	X	C and D	May be included as unstructured information for limited request types*
Foreign activities	X	C and D	Required for limited request types such as S-visas*

(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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	May be included as unstructured information in supporting documentation for requests*
Juvenile criminal records information	X	C and D	May be included as unstructured information for limited request types*
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	May be included as unstructured information for limited request types*
Whistleblower, e.g., tip, complaint or referral	X	C and D	May be included as unstructured information for limited request types *
Grand jury information	X	C and D	May included as unstructured information for limited request types*
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C and D	May be included as unstructured information in supporting documentation for requests*
Procurement/contracting records			
Proprietary or business information	X	C and D	May be included as unstructured information in supporting documentation for requests*
Location information, including continuous or intermittent location tracking capabilities	X	C and D	May be included as unstructured information in supporting documentation for limited types of requests*
Biometric data:			
- **Photographs or photographic identifiers**	X	C and D	May be included as unstructured information for limited request types*
- **Video containing biometric data**			
- **Fingerprints**	X	C and D	May be included as unstructured information for limited request types*
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	C and D	May be included as unstructured information for limited request types*

(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
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	x	A	
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	x	A	
- **Queries run**			
- **Content of files accessed/reviewed**	x	A	
- **Contents of files**			
Other (please list the type of info and describe as completely as possible): Professional Contact Information	X	A, B, and C	E-mail address, phone number and mailing address of the law enforcement personnel or attorney submitting the request*
Other:	X	A, B, C, and D	The presence of information is entirely dependent on the circumstances of each individual case. Because of the varied nature of the Division's work, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system. The information would relate to the defendant(s), witness(es) or other subject(s) involved in an investigation. With the exception of name, location and occasionally date of birth, none of the information listed above is specifically solicited by this system, but to the extent it is present within a case description or supporting documentation, it can be indexed and searched by SAS.

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):		

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

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	☒	☐	☒	Direct Access will be granted to authorized employees within OEO with valid user permissions. Entities submitting applications or requests will have direct log-in access, limited strictly to the initial submission and progress monitoring for their individual requests.

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	☒	☐	☒	Requestors in the USAOs will have direct log-in access, limited strictly to the initial submission and progress monitoring for their individual requests. Other DOJ components will not have direct access to this system and their results will be shared with the requestor.
Federal entities	☒	☐	☐	The results of the request will be shared with the requestor.
State, local, tribal gov't entities	☐	☐	☐	
Public	☐	☐	☐	
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	☒	☐	☐	In specific instances where appropriate to the type of request, the results may be shared with counsel or the courts. Additional information may be shared with involved parties or defendants through the judicial discovery process.
Private sector	☐	☐	☐	
Foreign governments	☐	☐	☐	
Foreign entities	☐	☐	☐	
Other (specify):	☒	☐	☐	Reports to officials outside of the Department (e.g., Congress) concerning Division caseload, activities, performance, and needs.

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 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.

Individuals are provided with general notice of the existence of case files through the Division System of Record Notice (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) and SORN CRM-022, Witness Immunity Records last published in full at 52 Fed. Red 47200 (Dec. 11, 1987) and amended at 82 Fed. Reg. 24147 (May 25, 2017).

Individuals are not provided with specific or direct notice of collection about themselves, as it may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation.

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.

Individuals are not provided with opportunities to participate in the collection, use or dissemination of information in the system, because the disclosure of the information may jeopardize 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.

Individuals who are the subject of the records will not be provided access or amendment capabilities to the records in SAS as doing so may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation. Information in this system is exempt from the access, amendment, correction, and notification procedures of the Privacy Act, as articulated in the chart available at https://www.justice.gov/opcl/doj-systems-records#CRM.

Individuals may make access requests for information maintained in this system via the Freedom of Information Act (FOIA). Such requests will be processed according to the provisions of the FOIA.

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):** For security compliance purposes, SAS is an application of the Custom Database Application System (CDAS), for which the current ATO expires on October 18, 2023. **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's Cyber Security Assessment and Management (CSAM) tool. 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:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** As a sub-system of Custom Database Applications System (CDAS), the system has undergone assessments, penetration tests, vulnerability scans, and is monitored by other means by the Division Information Systems Security Officer.
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:** 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. Information Owner/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 (CRM Template) may have reports designed to monitor for unusual activity. These reports would be reviewed on the basis determined by the business/information owner.

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:** Training specific to this system will be conducted for all authorized OEO users prior to the launch of SAS, and one-on-one training will be provided to newly authorized users after that point. The system is designed to function intuitively for requestors; however, telephone support is provided should questions arise.

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 measures to reduce the risk of compromise to PII. 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:

- SAS is a sub-system of the Custom Database Application System (CDAS). CDAS has a security categorization of FISMA Moderate and has selected the applicable security controls for a Moderate baseline.[32] The Division will ensure that SAS only solicits information categorized as Medium- or Low-Impact under NIST FIPS Publication 199 and NIST SP 800-60, Volume II publications and that no data fields solicit "High-impact" information without specifically granted approval from appropriate privacy and security personnel, to ensure adequate controls are applied to protect such information.[33]
- The system is accessible by Departmental 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 employee's 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,

[32] Per NIST SP 800-60, Vol. II, a Moderate-impact system is one in which the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals, *see* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf.

[33] Per NIST SP 800-60, Vol. II, a High-impact system is on in which the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals, *see Id.*

encryption, and other technical controls in accordance with applicable security standards.

- As described throughout this PIA, all SAS users must complete annual CSAT training, as well as read and agree to comply with Departmental information technology Rules of Behavior. CDAS 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/role-based 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, CDAS'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 SAS will conform to processes and procedures established by the Criminal Division Records Management Section (RMS) for the disposition of hardcopy and softcopy records. Presently, each of the record types listed under 2.1, has an individual records retention schedule. The Division is presently reviewing each of those records schedules to assess their suitability for the media-neutral requirements being enacted throughout the federal government, appropriate retention time in accordance with current needs and the inclusion in the SAS database. At the conclusion of the review, the Division will most likely choose to develop a single National Archives and Records Schedule encompassing each record type, as opposed to updating the existing individual records schedules. Because the National Archives currently has a minimum two-year waiting time for record schedule approvals, the Division cannot anticipate the date of completion. These records will be retained permanently until such time as the records retention schedule is approved.

The present retention schedules are:

Portfolio	Retention Schedule	Destruction Schedule
Consultations or Authorizations to Apply for Warrants to Search the Premises or Property of Subject Attorneys - Case Files	N1-060-03-001/ 1	10 years
Consultations or Authorizations to Apply for Warrants to Search the Premises or Property of Subject Attorneys - Master Files	N1-060-08-022	10 years
Issuance of Subpoenas to Attorneys for Information Relating to the Representation of Clients - Case Files	N1-060-03-001/ 1	10 years
Issuance of Subpoenas to Attorneys for Information Relating to the Representation of Clients - Master Files	N1-060-08-022	10 years
Use of Classified Investigative Technologies	Pending	Permanent

Courtroom Closures	N1-060-96-005	3 years
Multi-District (Global) Plea Agreements	N1-060-03-001/ 5	10 years
Nolo Contendere Pleas	Pending	Permanent
Alford Pleas	Pending	Permanent
Notices of Intent to Prosecute Attorneys	Pending	Permanent
Dual and Successive Prosecution Policy ("Petite Policy") Waivers	N1-060-03-001/ 4	10 years
Special Grand Jury Certifications	N1-60-96-5	5 years
Touhy Requests	N1-060-88-011 - 233279	Multi-section cases are permanent. Single section cases are 15 years.
Indictments for Unlawful Flight to Avoid Prosecutions	N1-060-88-010 - Class 126	Multi-section cases are permanent. Single section cases are 10 years.
Approval to Compel Testimony (Witness Immunity) - Case Files	N1-060-03-001/ 2	20 years
Approval to Compel Testimony (Witness Immunity) - Master Files	N1-060-08-016	20 years
Requests for Special Confinement Procedures (Special Administrative Measures)	Pending	Permanent
"S"- Nonimmigrant Visas - Master File	N1-060-08-013	Destroy ten years after close of case.
"S"- Nonimmigrant Visas - Case File	N1-060-04-006	Significant cases are retained permanently.
"S"- Nonimmigrant Visas - Case File	N1-060-04-006	Non-significant cases - Destroy ten years after close of case.
Sensitive Consensual Monitoring	Pending	Permanent
Re-subpoenaing a Previously Contumacious Witness before Successive Grand Juries	N1-060-03-001/ 5	10 years
Confidential Disinterested Third-Party Search Warrants	Pending	Permanent
Declining to Prosecute Failure to Register with the Selective Service System	N1-060-88-010 Class 25	Multi-section case files are permanent, Single-section case files - 10 years
Prosecution after a Compulsion Order (Previously Immunized Witness)	N1-060-03-001/ 5	10 years
News Media Policy Consultations	Pending	Permanent
Issuance of Subpoenas to a Member(s) of the News Media	N1-060-96-005	10 years
Use Subpoenas, 2703(d) or 3123 Orders to Obtain the Communications Records or Business Records of a Member of the News Media	N1-060-96-005	10 years

Application for warrants to search the premises, property, communications records, or business records of members of the news media	N1-060-96-005	10 years
Requests for authorization to charge or arrest a member(s) of the news media	N1-060-96-005	10 years
Requests for authorization to question members of the news media	N1-060-96-005	10 years
Requests for Retrocession/Acquisition of Federal Jurisdiction	N1-060-88-011 - 235033	Permanent - transfer to archives after 30 years
Certain Requests for Non-Prosecution or Deferred Prosecution	Pending	Permanent
Requests for Authorization to Exercise Law Enforcement Powers by Offices of the Inspector General	Pending	Permanent
Utilization of Persons in Custody of BOP or USMS for Investigative Purposes, or as Targets of Investigative Activity	Pending	Permanent
Electronic Surveillance - Master File	N1-060-08-015	Master File - Delete 10 years after expiration of request.
Electronic Surveillance - Case File	N1-060-88-010 Class 177	Case Files - Multi-section files are permanent, single section files are destroy in 10 years after close
Closed Circuit Television Monitoring - Master File	N1-060-08-015	Master File - Delete 10 years after expiration of request.
Other unique special techniques which may develop, in which the Department believes may warrant special review in order to assure compliance with legal of Departmental regulations	Case specific	Permanent until a records retention is identified or developed

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:

System of Records Notice 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/CRM-022, Witness Immunity Records last published in full at 52 Fed. Reg. 47200 (Dec. 11, 1987) and amended at 82 Fed. Reg. 24147 (May 25, 2017); and

SORN JUSTICE/DOJ-002, DOJ Computer Systems Activity & Access Records, 64 Fed. Reg. 73585 (Dec. 30, 1999), 66 Fed. Reg. 8425 (Jan. 31, 2001), 82 Fed. Reg. 24147 (May 25, 2017).

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?

Privacy Risk: Unauthorized access or misuse of information.

Mitigation: The Department employs a robust physical security system to protect its servers and access terminals, including secure worksites, armed guards, cameras, and access restricted office suites. CDAS also implements access monitoring, 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 delimited 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 the FISMA.[34] An audit log is maintained of all user logins and actions. Notification of the monitoring is presented clearly when logging into the system. JSOC oversees the audits of this system.

Additionally, Department employees and contractors must complete annual training regarding the handling of information as part of the Department's Cyber Security and Awareness Training (CSAT), as well as read and agree to comply with Departmental Information Technology Rules of Behavior. This occurs during their orientation upon entering into service with the Department, and annually thereafter. Additionally, OEO plans to provide training for employees granted access to SAS upon the implementation of the database, and one-on-one training for specific user-roles or new employees. The Division maintains an Account Management Guide and Configuration Management Guide for SAS.

The IT system assessment is documented in the CSAM assessment tool and maintained as part of the Department's ongoing authorization and assessment plan. All security controls are documented in the System Security and Privacy Plan recorded in the IT system. Only DOJ users may access the system; more specifically, users within the Criminal Division and certain members of U.S. Attorneys' Offices who are provided updates about information in the system

[34] Pub. L. 113-283, 128 Stat 3073 (2014).

(but cannot access the system to gain additional information). Administrator access is restricted to the few Division 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 criminal investigation, the mere presence of a name in the system can generate the assumption of involvement with criminal activity or other damage to reputation. For this reason, there is no automated dissemination of information from this system outside of the Department. Any dissemination must be done pursuant to proper authority and management review. Some information contained in this system is considered law enforcement sensitive; where the Division must make reference to classified investigative technologies, it will not input any classified information into the system.

Additionally, SAS contains a name search restriction that can be applied by management to specific cases, where the nature or subject of the investigation may be particularly sensitive. This restriction prohibits all but management, approving officials, and the attorney conducting the legal analysis for the case to view the subject's name or access case information or uploaded case materials.

Finally, de-identification of management reporting is practiced in all instances possible. Therefore, when reports are generated, they do not contain PII.

Privacy Risk: Over-collection.

Mitigation: Because criminal investigations and prosecutions are continually evolving endeavors, it is not always possible to know whether collected information will be relevant or necessary as a matter matures. In order to mitigate these concerns, the Division considered the careful minimization of information collection in the design of SAS. Each type of special technique request (as listed above in Section 1(a)) has a customized data entry interface that solicits the minimal amount of information required to perform the necessary analysis and due diligence records checks. The system solicits and collects the minimum amount of required information through structured text fields to help limit the possibility of over-collection.[35] Only those few special technique types with a verified need for the collection of information such as DOBs, FBI#s, USMS#s, BOP#s, or immigration-related information solicit that information.

Privacy Risk: Erroneous or inaccurate information.

Mitigation: Based on the sensitive investigative nature of these records, members of the public cannot enter records directly into the system or access it for review. Information in this system is obtained through investigative agencies and prosecutorial or court documents. Both the submitter of the request and OEO personnel have a substantial interest in ensuring the accuracy of the information in this system. Both the investigating agency(ies) and the Department verify

[35] Each free text field has a description of what should be entered into it. These are aimed at articulating the elements of the offenses and why the particular investigative action is necessary.

this information as part of the normal procedures associated with day-to-day tasks, which include multiple levels of oversight and review. Every effort is made to diligently review, verify, and correct information from these records. Investigations and prosecutions are conducted in the timeliest manner possible based on the variables and complexities of each case. Additionally, this database has built in requirements for the submitter to certify that they have read the relevant Departmental policy regarding that specific type of request and to certify that the request has been reviewed and authorized by the appropriate supervisory official.