Federal Bureau of Investigation

Privacy Impact Assessment
for the
[Combined National Deoxyribonucleic Acid (DNA) Index System (CODIS)]

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

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

Date approved: 3/14/2023

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Combined Deoxyribonucleic Acid (DNA) Index System (CODIS) provides a local, state and federal tiered search and storage capability for DNA Records submitted by participating Criminal Justice Agency forensic laboratories and Criminal Justice Booking Agencies.[1, 2] CODIS allows users to search these DNA Records to identify crime scene offenders, missing persons, or unidentified human remains, or to link multiple crime scenes. CODIS utilizes the FBI's Criminal Justice Information Services (CJIS) Shared Enterprise Network (SEN) and Wide Area Network (WAN) to enable communications between and among the local, state and federal CODIS tiers.[3] All individuals with access to CODIS are assigned a unique Username, Identification Number and initial password by the FBI Laboratory Division's CODIS Unit, and must successfully pass a limited FBI background investigation, which consists of a continuous fingerprint check for arrests and convictions.

Section 208 of the E-Government Act of 2002, P.L. 107-347 requires that agencies conduct Privacy Impact Assessments (PIAs) on information technology systems that collect and maintain identifiable information regarding individuals, and, if practicable, to make such PIAs publicly available. Accordingly, this PIA has been conducted and will be made publicly available. As changes are made to CODIS, this PIA will be appropriately reviewed and revised.

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

---

[1] A Criminal Justice Agency is an agency or institution of the federal, state, or local government, other than the office of the public defender, which performs, as part of its principal function, activities relating to the apprehension, investigation, prosecution, adjudication, incarceration, supervision or rehabilitation of criminal offenders. A Criminal Justice Booking Agency is a Criminal Justice Agency with the authority to perform booking activities. Where permitted by state law, such agencies will conduct a Rapid DNA test at the time of booking to identify if the arrestee is associated with unsolved crimes. Rapid DNA (or "swab-in – profile-out") test instruments meet the FBI standards for Rapid DNA submission, but are directly purchased from commercial vendors by the Criminal Justice Booking Agency and are outside the CODIS system boundary. Rapid DNA test results can be obtained within two hours.

[2] As CODIS is multijurisdictional, the FBI has exclusive authority only over those CODIS records that are uploaded to a CODIS installation operated by the FBI. Such installations and records will be described in this document as *FBI CODIS* and defined in Section 2.1. This document will describe CODIS broadly when possible, and FBI CODIS specifically when necessary.

[3] CJIS SEN and WAN are subject to separate privacy documentation, as required. Rapid DNA test instruments are used in tandem with a bidirectional portal, also known as the CODIS Rapid Enrollment Application (CREA), and the CJIS SEN and WAN, to transmit and receive information to/from the applicable Criminal Justice Agency forensic laboratory. Neither CREA nor the CJIS SEN and WAN store any information.

previously unknown areas of concern or patterns.

CODIS utilizes a three-tiered index system to organize DNA information and create a national search and storage capability for DNA Records. The first (and lowest level) of CODIS's three tiers consists of Local DNA Index Systems (LDISs), which generally correspond with city and county participating Criminal Justice Agency forensic laboratories.[4] The second tier consists of State DNA Index Systems (SDISs),[5] which generally correspond with participating Criminal Justice Booking Agencies (for arrestee Rapid DNA testing) and state-level Criminal Justice Agency forensic laboratories. The third tier is the National DNA Index System (NDIS), which is comprised of all permissible LDIS and SDIS DNA Records. DNA Records flow upward from LDISs to SDISs, which enables forensic laboratories within the state to compare DNA Records; and from SDISs to NDIS, which enables forensic laboratories to compare DNA Records on a national level.

The FBI LDISs, FBI SDIS and NDIS (collectively, FBI CODIS) servers and software configurations are wholly controlled and operated by the FBI. In contrast, state, local and other federal participating Criminal Justice Agency forensic laboratories retain control of CODIS server and software configurations within their respective entities. Similarly, Criminal Justice Booking Agencies, which do not have login access to CODIS, are responsible for the network infrastructure required to send data through the CJIS SEN and WAN to their respective SDIS. However, to participate in NDIS, all entities must meet quality assurance and proficiency testing standards issued by the FBI under 34 U.S.C. § 12591, pursuant to the Federal DNA Identification Act, 34 U.S.C. § 12592.[6] In addition, to be eligible for NDIS, DNA Records must be indexed into one of the following eight permissible categories:

(1) Persons convicted of crimes;

(2) Persons who have been charged in an indictment or information with a crime;

(3) Non-United States Persons who are detained under the authority of the United States;

---

[4] In addition to state and local LDISs, the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) maintain respective LDISs. The ATF LDIS contains DNA Records from ATF investigation crime scenes. The FBI LDISs contain DNA Records from FBI investigation crime scenes, federal arrestees, District of Columbia convicted offenders, and non-United States Person detainees (processed by the respective federal agency with appropriate jurisdiction).

[5] In addition to state and local SDISs, the FBI maintains a SDIS for DNA Record submissions by the FBI and ATF LDISs.

[6] The Federal DNA Identification Act, Id., required the formation of a DNA Advisory Board (DAB), a panel of distinguished professionals from both the public and private sectors, to address issues relevant to forensic DNA applications and laboratories. As a result of the DAB's work, *Quality Assurance Standards for Forensic DNA Testing Laboratories* and *Quality Assurance Standards for DNA Databasing Laboratories* were issued by the Director of the FBI in October 1998 and April 1999, respectively. Both documents have become benchmarks for assessing the quality of practices and performances of DNA laboratories throughout the country. Revisions to these standards are issued regularly by the FBI Director based upon recommendations from the Scientific Working Group on DNA Analysis Methods, the successor to the DAB. The Federal DNA Identification Act, Id., also required that the FBI Laboratory Division ensure that all DNA laboratories that are federally operated, receive federal funds, or participate in NDIS demonstrate compliance with these standards through annual internal audits and periodic external audits, at least every two years.

(4) Other persons whose DNA samples are collected under applicable legal authorities;

(5) Missing persons;

(6) Relatives of missing persons;

(7) Unidentified persons; or

(8) Persons whose identities are not known with certainty and who left DNA at the scene of a crime.

Within the eighth index (*Persons whose identities are not known with certainty and who left DNA at the scene of a crime*) is the DNA Index of Special Concern (DISC) subcategory. DISC contains DNA Records developed from unsolved homicide, rape, sexual assault, kidnapping, and terrorism cases.

Records that do not meet FBI index, quality assurance and one of the eight permissible category requirements will be automatically rejected by NDIS upon attempted upload.

All DNA Records in CODIS contain a DNA profile[7] of the individual (or for missing persons, a DNA pedigree[8] of their biological relatives), and the Metadata required to manage and operate CODIS. For Criminal Justice Agency forensic laboratory submissions to NDIS, the CODIS Metadata typically consists of the Originating Forensic Laboratory Identifier (ORI), which is assigned by CJIS, a Specimen Identification Number, and the CODIS Username associated with the submission of the DNA profile. However, for Criminal Justice Agency forensic laboratory submissions for the NDIS DISC index subcategory, and for Criminal Justice Booking Agency Submissions to SDISs, additional CODIS Metadata is provided.

For Criminal Justice Agency forensic laboratory submissions for the NDIS DISC index subcategory, the following additional CODIS Metadata is provided:

- Investigative Agency Identifier (INI), which is assigned by CJIS;
- Investigative Case Tracking ID, which is the investigative agency's reference tracking number for the case that yielded the evidence item;
- Investigative Case Alias (optional), which is the name sometimes given to notorious or serial crimes by investigative agencies;
- Investigator Email Address (optional), which is the email of the individual or department designated by the investigative agency as the point of contact for the case;

[7] A DNA profile is an individual's genetic constitution at defined locations (also known as loci) in the DNA.

[8] DNA pedigrees contain genetic information from two or more biological relatives of missing persons.

- Investigator Phone Number, which is the telephone number of the individual or unit/department designated by the investigative agency as the point of contact for the case;

- Statute of Limitations, which is the charge filing deadline for the crime associated with the evidence item;

- Offense Description, which is a description of the crime that yielded the evidence item;

- Extradition Information, which describes whether extradition is applicable; and

- Investigative Agency Contact Information, which contains any additional contact information or comments, but, by policy, may not contain any personally identifiable information (PII) of the victim.

For Criminal Justice Booking Agency submissions to SDIS, the following additional CODIS Metadata is provided:

- Booking Agency Identifier, which is assigned by CJIS;

- State Identification Number/Universal Control Number (identifies the state or federal arrestee, respectively);

- Fingerprint Event Identifier;

- Arrest Date;

- Fingerprint Capture Date/Time; and

- Offense Description.

Participating Criminal Justice Agency forensic laboratory users upload DNA Records into the appropriate LDIS/SDIS index within CODIS. Similarly, approved Criminal Justice Booking Agency users upload arrestee DNA Records into the corresponding SDIS within CODIS, via the CJIS SEN and WAN and an FBI-approved Rapid DNA instrument. Any record uploaded into CODIS that fits into one of the permissible categories and contains a DNA specimen that does not trigger a specimen reject rule (e.g., for minimum number of DNA loci or maximum number of DNA contributors), will be automatically marked for upload to NDIS. Users are notified at the time of upload if the record was accepted or rejected by NDIS.

NDIS automatically searches all submitted DNA Records, whether the record originated at a participating Criminal Justice Agency or a Criminal Justice Booking Agency, daily, to identify potential matches. If a potential match is identified during a daily search, CODIS generates a "match report," which contains the ORI, Specimen ID, CODIS Username, and DNA profile of the potential match or matches. The match report is automatically sent to the relevant participating Criminal Justice

Agency forensic laboratory through CODIS.

In addition to daily searches, for Criminal Justice Booking Agencies only, NDIS immediately searches the DISC index subcategory. If a match is identified during this search, CODIS utilizes NDIS information in conjunction with Criminal Justice Booking Agency information retained in the SDIS tier to generate an "Unsolicited DNA Notification" (instead of a "match report"). This notification is sent via the CJIS SEN and WAN to the Criminal Justice Booking Agency as well as the Criminal Justice Agency (or Agencies) that submitted the unknown DNA Record(s), and contains the INI, BNI, State Identification Number/Universal Control Number, Offense Description, Offense Description(s) of matched crime(s) in NDIS, and investigative agency contact information.

As NDIS does not store State Identification Number/Universal Control Number or otherwise collect, handle, disseminate, or store contributors' names, only participating Criminal Justice Agency forensic laboratories can confirm a match.

Access to CODIS is limited to participating Criminal Justice Agency forensic laboratories and authorized Criminal Justice Booking Agencies (using Rapid DNA instruments), for criminal law enforcement identification purposes only. There are three categories of users: CODIS Users, Criminal Justice Booking Agency Users, and IT Personnel Users.

- CODIS Users are Criminal Justice Agency forensic laboratory users. CODIS Users are authorized to add records, and to modify or delete records previously added by their Criminal Justice Agency forensic laboratory. CODIS Users cannot modify or delete the records of another Criminal Justice Agency forensic laboratory or Criminal Justice Booking Agency. CODIS Users are assigned a unique Username, Identification Number and initial password by the FBI Laboratory Division's CODIS Unit. CODIS Users may retrieve records from CODIS by ORI, INI, BNI, Specimen Identification Number, or their User Identification Number, but only to inspect, modify, or delete the DNA Records they are associated with uploading.

- Criminal Justice Booking Agency Users do not have logon access to CODIS. They can submit DNA Records and receive Unsolicited DNA Notifications through the CJIS SEN and WAN only. CJIS SEN and WAN access is provided independent of CODIS.

- IT Personnel Users are IT employees, contractors and detailees (personnel) at the FBI and Criminal Justice Agency forensic laboratories that have been given CODIS access for system and network maintenance purposes only. Such individuals are subject to the same access and background investigation requirements as standard CODIS Users, but do not have access permissions to add, edit or delete DNA Records. IT Personnel Users are assigned a unique Username, Identification Number and initial password by the FBI Laboratory Division's CODIS Unit.

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	34 U.S.C. §40702(a); 34 U.S.C. §12592.
Executive Order	
Federal regulation	28 C.F.R. § 28.12; 28 C.F.R. § 0.85.
Agreement, memorandum of understanding, or other documented arrangement	To participate in CODIS: • Criminal Justice Agency forensic laboratories must sign Memorandums of Understanding (MOUs) with the FBI. • Criminal Justice Booking Agencies must sign MOUs with their respective SDISs. These MOUs set forth the confidentiality, data access, and quality assurance standards required by the FBI pursuant to the Federal DNA Identification Act, Id..
Other (summarize and provide copy of relevant portion)	

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	CODIS Username, provided only for personnel authorized to submit records to CODIS
Date of birth or age	X	C & D	Missing persons descriptive metadata
Place of birth			
Gender	X	C & D	Missing persons descriptive metadata
Race, ethnicity or citizenship	X	C & D	Missing persons descriptive metadata
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
E-mail addresses (personal, work, etc.) Please describe in Comments			
Phone numbers (personal, work, etc.) Please describe in Comments			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			

(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
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	C & D	Missing persons descriptive metadata
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**	X	B*, C & D	*DNA is collected for certain military criminal offenses.
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A, B & C	
- **User passwords/codes**			
- **IP address**	X	A	
- **Date/time of access**	X	A	

(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
- **Queries run**	X	A	
- **Content of files accessed/reviewed**	X	A	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):			
- **ORI/INI/BNI**	X	A, B, & C	
- **Specimen Identification Number**	X	A, B, & C	
- **Identification Number for personnel authorized to submit DNA Records to NDIS**	X	A, B, & C	
- **Start/End Dates for personnel authorized to submit DNA Records to NDIS**	X	A, B, & C	
- **Missing Person Descriptive Metadata**	X	C & D	
- **DNA Pedigree**	X	C & D	
- **Investigative Case Alias**	X	C & D	
- **Investigator Email Address**	X	A, B, & C	
- **Investigator Phone Number**	X	A, B, & C	
- **Statute of Limitation**	X	C & D	
- **Offense Description**	X	C & D	
- **Extradition Information**	X	C & D	
- **Investigative Agency Contact Information**	X	A, B, & C	
- **State Identification Number/Universal Control Number**	X	C & D	

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		Hard copy: mail/fax		Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
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.

The FBI can only access and share FBI CODIS information.

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		X	Information is retrieved within the FBI via direct log-in as described in Section 2.1. On a case by case basis, information may be further disseminated within the FBI for law enforcement purposes, pursuant to the FBI's legal authorities.
DOJ components	X		X	Information is retrieved by DOJ components that are participating Criminal Justice Agencies, via direct log-in as described in Section 2.1. On a case by case basis, information may be further disseminated to such components for law enforcement purposes, as permitted by the applicable legal authorities.
Federal entities	X		X	Information is retrieved by Federal Entities that are participating Criminal Justice Agencies, via direct log-in as described in Section 2.1. On a case by case basis, information may be further disseminated to such entities for law enforcement purposes, as permitted by the applicable legal authorities.

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.**
State, local, tribal gov't entities	X		X	Information is retrieved by state, local, and tribal gov't entities that are participating Criminal Justice Agencies, via direct log-in as described in Section 2.1. Criminal Justice Booking Agencies do not have direct CODIS log-in access and cannot retrieve information on demand, but can receive Unsolicited DNA Notifications as described in Section 2.1. On a case by case basis, information may be further disseminated to such entities for law enforcement purposes, as permitted by the applicable legal authorities.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			On a case by case basis, as dictated by circumstances and permitted by the relevant legal authorities, information may be disseminated for litigation purposes.
Private sector				
Foreign governments	X			On a case by case basis, as dictated by circumstances and permitted by the relevant legal authorities, information may be disseminated to 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.

It is not anticipated that any FBI CODIS information will be released to the general public under the circumstances contemplated by this question.

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.

Notice of FBI collection, use, sharing and processing of CODIS information is provided pursuant to the following SORNS published in the Federal Register: *FBI Central Records System*, FBI-002, 63 Fed. Reg. 8671 (Feb. 20, 1998), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); and *National DNA Index System*, FBI-017, 61 Fed. Reg. 37495, amended by 66 Fed. Reg. 8425 (Jan 31, 2001), and 82 Fed. Reg. 24147 (May 25, 2017).

These SORNs provide general notice regarding the entities with and situations in which the FBI may use and disseminate the records that have been uploaded to FBI CODIS. The published routine uses and blanket routine uses applicable to these systems provide additional notice about the ways in which such CODIS information may be shared with other entities.

In addition, relatives of missing persons are required to sign a combined Consent and Privacy Act Statement. The relevant Privacy Act language states that providing a sample is voluntary but failure to provide a sample "may hinder the FBI's and other criminal justice agencies' abilities to assist in the identification of a kindred family member." The Statement further discloses how DNA samples will be used, as follows:

> The DNA analysis information will be released only to criminal justice agencies for identification and/or comparison to evidentiary items related to the investigation of the disappearance of individuals indexed in the Unidentified Human Remains Index of CODIS. Additionally, supplemental information, including the names and biological samples provided pursuant to this form, will be retained by the FBI separately from CODIS. Criminal justice agencies with access to CODIS may search the DNA analyses for DNA matches. If matches are found, the additional supplemental information may be released to those agencies in support of the purposes for which it was collected. The requested information may also be disclosed pursuant to routine uses listed in the Privacy Act system of records notices for the National DNA Index System and the FBI's Central Records System, as most recently published in the Federal Register.

Lastly, the *DOJ Information Technology, Information Systems, and Network Activity & Access Records*, DOJ-002, SORN, 86 Fed. Reg. 132 (July 14, 2021), is applicable to this system.

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.

Pursuant to the DNA Identification Act, 34 U.S.C. §12592, consent is not required to obtain a DNA sample from persons who are arrested, detained, or convicted. However, consent is required to collect and upload DNA records from relatives of missing persons to FBI CODIS.

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 may request their FBI CODIS records in accordance with the process set forth in the *National DNA Index System* SORN, 61 Fed. Reg. at 37497. Individuals may otherwise request CODIS records in accordance with applicable processes set forth by the relevant local, state and other federal notices/legal authorities.

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):** **Date of last ATO:** June 14, 2022 (FBI CODIS) **Date of ATO Expiration:** September 19, 2023 (FBI CODIS) **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:** There are no outstanding POAMs for any privacy controls resulting from the ATO process.
	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:

<table>
<tr><td>X</td><td>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:

<table>
<tr><td>Confidentiality</td><td>The system contains information that requires protection from unauthorized disclosure.</td><td>Moderate</td></tr>
<tr><td>Integrity</td><td>The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification.</td><td>Moderate</td></tr>
<tr><td>Availability</td><td>The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses.</td><td>Moderate</td></tr>
</table>
</td></tr>
<tr><td>X</td><td>Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:
The FBI follows NIST Risk Management Framework Special Publication 800-37 as the standard for the ATO process.</td></tr>
<tr><td>X</td><td>Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:
FBI CODIS maintains audit logs for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, and potential intrusion. These audit records are reviewed at least weekly by the NDIS Information System Security Officer. User accounts are disabled immediately when users are no longer actively employed within the program or are found to be using information inappropriately. In addition, FBI CODIS vulnerability scans are conducted weekly and as necessary to identify and mitigate weaknesses which may become exploited and lead to exfiltration of data collected.</td></tr>
<tr><td>X</td><td>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.
Contractors that have access to FBI CODIS 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.</td></tr>
<tr><td>X</td><td>Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel</td></tr>
</table>

	on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: All CODIS Users are required to undergo annual CODIS training specific to their user role, including annual training for DISC submissions.

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?

The key privacy and security administrative, technical, and physical controls for minimizing privacy risks are as follows:

- CODIS data is validated by manual comparison to source data.
- All communications within CODIS occur via secure protocols (FTPS/HTTPS) over the CJIS SEN and WAN, and are encrypted at the ingress CJIS router and decrypted at the egress CJIS router.
- Only authenticated and authorized CODIS users can view, create, or modify information in the system.
- Access to FBI CODIS is password protected and uses two-factor authentication.
- Access to CODIS is role-based. User groups are established based on a defined need to know and a role requiring access to the data.
- Only IT Personnel Users assigned to the FBI Laboratory Division, under specific instruction from the NDIS Custodian,[9] can physically access the FBI CODIS servers and make configuration changes to these CODIS instances.
- FBI CODIS is audited for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, and potential intrusion.
- FBI CODIS audit logs are reviewed at least weekly by the NDIS Information System Security Officer.
- CODIS user accounts are disabled immediately when users are no longer actively employed within the program or are found to be using information inappropriately.
- FBI CODIS vulnerability scans are conducted weekly and as necessary to identify and mitigate weaknesses which may become exploited and lead to exfiltration of data collected.
- FBI CODIS validates that records are complete and properly formatted before upload is permitted.
- CODIS Users and IT Personnel Users must successfully pass a limited FBI background investigation, which consists of a continuous fingerprint check for arrests and convictions.

[9] The NDIS Custodian is a senior FBI employee in the FBI CODIS unit. The NDIS Custodian is the person ultimately responsible for ensuring that Criminal Justice Agency forensic laboratories meet the requirements for participating in NDIS.

Lastly, for DNA records submitted to NDIS, established quality assurance procedures ensure:

- the specimen submission is from one of the permitted categories described above in Section 2.1;
- the specimen was processed using an acceptable DNA kit (or Rapid DNA instrument);
- the specimen does not violate the FBI's specimen reject rules (e.g. minimum number of DNA loci, interpretation rules, maximum number of DNA contributors); and
- the computer terminals/servers used for CODIS and the DNA indexes are in physically secured spaces, and login access to these computers is limited to only those individuals authorized to use CODIS and approved by the FBI, pursuant to the Federal DNA Identification Act.

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.)

The disposition of FBI CODIS information is described in the National Archives and Records Administration Job Number N1-065-06-9, *National DNA Indexing System*.

- System output will be destroyed upon termination of FBI CODIS.
- Policy, usage agreements and any MOUs between NDIS and participating Criminal Justice Agency forensic laboratories (which, via addendum, include Criminal Justice Booking Agencies) will be destroyed when superseded, obsolete, or upon termination of NDIS, whichever is sooner. (SDIS and LDIS MOUs that do not include the FBI as a party are subject to local, state, and other federal record disposition legal authorities.)
- Audit information will be destroyed when 25 years old.

State and local LDIS and SDIS information that has not been shared with NDIS is not FBI record information.

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.

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:

FBI Central Records System, FBI-002, 63 Fed. Reg. 8671 (Feb. 20, 1998), amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); and *National DNA Index System*, FBI-017, 61 Fed. Reg. 37495, amended by 66 Fed. Reg. 8425 (Jan 31, 2001), and 82 Fed. Reg. 24147 (May 25, 2017); *DOJ Information Technology, Information*

Systems, and Network Activity & Access Records, DOJ-002, 86 Fed. Reg. 132 (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.***

The type, quantity, and sources of information collected by FBI CODIS are necessary to identify crime scene offenders, missing persons, or unidentified human remains, or to link multiple crime scenes. Such information is only further disseminated for these purposes. Moreover, NDIS does not store State Identification Number/Universal Control Number or otherwise collect, handle, disseminate, or store contributors' names. Therefore, CODIS DNA profiles and pedigrees can only be matched to a named individual by the submitting Criminal Justice Agency forensic laboratory, independent of NDIS.

- The privacy risks associated with the collection and maintenance of FBI CODIS information are inaccurate information, unauthorized access, and unauthorized disclosures.
- The privacy risks associated with the access and use of FBI CODIS information are unauthorized access, unauthorized (or overly broad) disclosures, and loss of data.
- The privacy risks associated with the dissemination of FBI CODIS information are the risks of unauthorized disclosures and loss of data.

The risks of unauthorized access, unauthorized disclosures, loss of data and inaccurate information are mitigated by the quality assurance standards promulgated by the FBI[10] pursuant to the Federal DNA

[10] *See "*Quality Assurance Standards for Forensic DNA Testing Laboratories" and the "Quality Assurance Standards for DNA Databasing Laboratories" https://le.fbi.gov/science-and-lab-resources/biometrics-and-fingerprints/codis#Quality-Assurance. These were first issued by the Director of the FBI in October 1998 and April 1999, respectively. The DNA Identification Act of 1994 also required that the FBI Laboratory ensure all DNA laboratories that are federally operated, receive federal funds, or participate in the National DNA Index System (NDIS) demonstrate compliance with the standards issued by the FBI. Typically, documentation of a laboratory's compliance with a stated standard has been measured through an audit process.

Identification Act. These risks are further mitigated by the system, physical access, network-infrastructure, auditing and quality assurance controls, as described more specifically in Sections 6.1 and 6.2, which are in compliance with FIPS Publication 199, as applicable.

The risk of inaccurate information is also specifically mitigated through the identity verification process performed by participating Criminal Justice Agency forensic laboratories to confirm a potential match. The identity must be confirmed prior to the disclosure of any personally identifiable information to the law enforcement entity who submitted the DNA sample.

Lastly, notice is provided as described in Section 5.1.