Federal Bureau of Investigation

Privacy Impact Assessment
for the
[National Deoxyribonucleic Acid (DNA) Index System (NDIS) of the Combined DNA Index System Software (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: September 27, 2022

(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 National Deoxyribonucleic Acid (DNA) Index System (NDIS) is a national index of permissible DNA records input by federal, state and local participating Criminal Justice Agency[1] forensic laboratories. The permissible record categories are described in Section 2. These records can be searched using the FBI's Combined DNA Index System software (CODIS), to identify crime scene offenders, missing persons, or unidentified human remains, or to link multiple crime scenes.

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 NDIS, 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 previously unknown areas of concern or patterns.

NDIS is a national index of DNA records input by federal, state and local participating Criminal Justice Agency forensic laboratories. These records can be searched using CODIS, to identify crime scene offenders, missing persons, or unidentified human remains, or to link multiple crime scenes.[2]

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. The second tier consists of State DNA Index Systems (SDISs), which generally correspond with state-level participating Criminal Justice Agency forensic laboratories. 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

---

[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. To participate in NDIS, a Criminal Justice Agency forensic laboratory must sign a Memorandum of Understanding with the FBI, which sets forth confidentiality, data access, and quality assurance standards.

[2] CODIS is discussed in detail throughout this document, because it is the means by which users access NDIS. CODIS may be the subject of separate privacy documentation, as required.

laboratories to compare DNA records on a national level.[3] Criminal Justice Agency forensic labs that are authorized to participate in NDIS are assigned an Originating Agency Identifier (ORI) by the FBI's Criminal Justice Information Services (CJIS) division.

Each DNA record contains only a DNA profile[4] (or DNA pedigree[5] for missing persons) and the data required to manage and operate NDIS, i.e., the ORI, the Specimen Identification Number, and the CODIS username associated with the submission of the DNA profile. DNA records must describe one of the following permissible categories to be accepted into NDIS:[6]

- Persons convicted of crimes;
- Persons who have been charged in an indictment or information with a crime;
- Non-United States Persons who are detained under the authority of the United States;
- Other persons whose DNA samples are collected under applicable legal authorities;
- Missing persons;[7]
- Relatives of missing persons;
- Unidentified persons; and
- Persons whose identities are not known with certainty and who left DNA at the scene of a crime.

Participating Criminal Justice Agency forensic laboratory users upload DNA records into their respective LDIS or SDIS indexes within CODIS. If the DNA record fits into one of the permissible categories and the DNA specimen does not trigger a specimen reject rule (e.g., for minimum number of DNA loci or maximum number of DNA contributors) it is automatically marked for upload to NDIS. Otherwise, the record will be rejected by NDIS. Users are notified at the time of upload if the record was accepted or rejected.

NDIS is automatically searched daily, Monday through Friday, to identify potential matches. Searches that result in a potential match, generate a "match report" that 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 users through CODIS. The participating Criminal Justice Agency forensic laboratory is responsible for confirming the match independent of NDIS.[8]

NDIS does not contain DNA samples or the names of DNA contributors. NDIS contains DNA profiles, DNA pedigrees and certain contributor discriptors other than name, as described in Section 3. NDIS also includes the names of federal, state, and local employees, contractors and detailees

---

[3] LDIS and SDIS are subject to separate privacy documentation.

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

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

[6] These categories are authorized by the Federal DNA Identification Act, 34 U.S.C. §12592.

[7] The missing person category also contains metadata (e.g., physical characteristics, gender, age, date of birth, date of last contact, and last known location) to assist in the identification of unidentified remains. Metadata is not permitted to be used for any other category. Federal DNA Identification Act, Id. at §12592(a).

[8] Because NDIS does not collect, handled, disseminate, or store contributor name, only participating Criminal Justice Agency forensic laboartories can confirm a match.

(personnel) authorized to submit DNA records to NDIS, and their authorized start and end dates, to facilitate interagency communications and ensure record integrity. CODIS, which is used to access NDIS, collects and maintains user logon and activity records of CODIS users to NDIS, and their authorized start and end dates, to facilitate interagency communications and ensure record integrity. CODIS, which is used to access NDIS, collects and maintains user logon and activity records of CODIS users.

In accordance with the Federal DNA Identification Act, 34 U.S.C. §12592(a), access to NDIS is limited to participating Criminal Justice Agency forensic laboratories for law enforcement identification purposes only.

To obtain access to NDIS (which is only accessible via CODIS), individuals must be employed at a participating Criminal Justice Agency forensic laboratory and must successfully pass an FBI background investigation for Secret security clearance. Approved users are assigned a unique username, identification number and initial password by the FBI Laboratory Division's CODIS Unit. There are two broad categories of users: standard CODIS users, and IT personnel users.

- Standard CODIS users have the ability to add records, and to modify or delete records previously added by their Criminal Justice Agency forensic laboratory. Standard CODIS users cannot modify or delete the NDIS records of another Criminal Justice Agency forensic laboratory. Standard CODIS users may retrieve NDIS records by ORI, NDIS Specimen Identification Number, or their unique identifier, but only to inspect, modify, or delete the DNA records they are associated with uploading.

- IT personnel at the FBI and Criminal Justice Agency forensic laboratories may be 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.

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 NDIS, a Criminal Justice Agency forensic laboratory must sign a Memorandum of Understanding (MOU) with the FBI, which sets forth confidentiality, data access, and quality assurance standards.
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	Names are only included for personnel authorized to submit records to NDIS
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			

(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
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			
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)**			

(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
System admin/audit data:			
- **User ID**	X	A, B & C	
- **User passwords/codes**			
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **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**	X	A, B, & C	
- **Specimen Identification Number**	X	A, B, & C	
- **Identication 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	

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

Government sources:					
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.

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, as a participating Criminal Justice Agency, via direct log-in, as described in Section 2.1. On a case by case basis, information may be further disseminated within and outside the FBI for law enforcement purposes, pursuant to the FBI's 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.**
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 by such components for law enforcement purposes, pursuant to the component's 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 by such entities for law enforcement purposes, pursuant to the entity's legal authorities.
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. On a case by case basis, information may be further disseminated by such entities for law enforcement purposes, pursuant to the entity's 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 circumscribed by the relevant legal authorities, information may be disseminated for litigation purposes.
Private sector				
Foreign governments				
Foreign entities				

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.
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 NDIS data 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 is provided pursuant to the following system of records notice published in the Federal Register: *FBI Central Records System*, 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*, 61 Fed. Reg. 37495, amended by 66 Fed. Reg. 8425 (Jan 31, 2001), and 82 Fed. Reg. 24147.

These SORNs provide general notice regarding the entities with and situations in which the FBI may use and disseminate the records in this system. The published routine uses and blanket routine uses applicable to this system provide additional notice about the ways in which information maintained by the FBI may be shared with other entities.

In addition, the DOJ Information Technology, Information Systems, and Network Activity & Access Records 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 USC 40702 (a)(4), consent is not required to obtain a DNA sample from persons who are arrested, detained, or convicted. However, consent is required for the collection and databasing of DNA from relatives of missing persons.

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 NDIS records in accordance with the process set forth in the *National DNA Index System* SORN, 61 Fed. Reg. at 37497.

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).

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

Date of ATO Expiration: September 19, 2022

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.</td></tr>
<tr><td></td><td>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:</td></tr>
<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>
</table>
</td></tr>
</table>

	Availability	The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses.	Moderate

X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The CODIS Unit follows National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) Special Publication (SP) 800-37 as the standard for the Assessment and Authorization (A&A) process.
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:** • CODIS maintains audit logs for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, and potential intrusion. CODIS audit records are reviewed at least weekly. User accounts are disabled immediately when users are no longer actively employed within the program or are found to be using information inappropriately.
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:** All individuals with access to NDIS are required to undergo annual CODIS training specific to their user role.

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:

- System data is validated by both manual and hash value comparison to source data.

- All communications to and from NDIS occur via secure file transfer protocol (FTP) over the FBI's CJIS Secure Enterprise Network (SEN).[9] All communications transmitted over the CJIS SEN are encrypted at the ingress CJIS router and decrypted at the egress CJIS router.
- Only authenticated and authorized users can view, create, or modify information in the system.
- Access to the system is password protected.
- Access to the system 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 assigned to the FBI Laboratory Division, under specific instruction from the NDIS Custodian,[10] can physically access the server and make configuration changes to the system.
- The system is audited for invalid login attempts, invalid session transactions, unusual patterns of use, malicious code, file integrity, and potential intrusion.
- Audit logs are reviewed weekly by the 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.
- Vulnerability scans are conducted monthly to identify and mitigate weaknesses which may become exploited and lead to exfiltration of data collected.
- The system validates that records are complete and properly formatted before upload is permitted.

Lastly, established quality assurance procedures ensure:

- that the specimen submission is from one of the permitted categories described above in Section 2.1;
- that the specimen was processed using an acceptable DNA kit;
- that 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
- that the computer terminals/servers used for CODIS and the DNA indexes are in physically secured spaces, and access to these computers is limited to only those individuals authorized to use CODIS and approved by the FBI.[11]

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and

---

[9] CJIS SEN is subject to separate privacy documentation, as required.

[10] 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.

[11] The Federal DNA Identification Act, Id. at §12592, 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 practices and performances of DNA laboratories throughout the country. Revisions to these standards are promulgated regularly by 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.

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 NDIS 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 NDIS.
- Policy, usage agreements and MOUs will be destroyed when superseded, obsolete, or upon termination of NDIS, whichever is sooner.
- Audit information will be destroyed when 25 years old.

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, 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*, 61 Fed. Reg. 37495, amended by 66 Fed. Reg. 8425 (Jan 31, 2001), and 82 Fed. Reg. 24147.

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 and used by NDIS are necessary for

participating Criminal Justice Agencies to identify crime scene offenders, missing persons, or unidentified human remains, or to link multiple crime scenes. NDIS information is only further disseminated for these purposes. Moreover, NDIS does not contain DNA samples or the names of DNA contributors. NDIS contains DNA profiles, DNA pedigrees, and certain contributor discriptors other than name, as described in Section 3, which can only be matched to a named individual by the submitting participating Criminal Justice Agency forensic laboratory, independent of NDIS.

- The privacy risks associated with the collection and maintenance of NDIS information are inaccurate information, unauthorized access, and unauthorized disclosures.
- The privacy risks associated with the access and use of NDIS information are unauthorized access, unauthorized (or overly broad) disclosures, and loss of data.
- The privacy risks associated with the dissemination of NDIS 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 system, physical access, network-infrastructure, auditing and quality assurance controls, as described more specifically in Sections 6.1 and 6.2. These mitigations 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 Agencies to confirm a potential match. The identify must be confirmed prior to the disclosure of any personally identifiable information to the law enforcement entity who submitted the DNA sample to the participating Criminal Justice Agency forensic laboratory.

Lastly, notice is provided as described in Section 5.1.