Federal Bureau of Investigation

Privacy Impact Assessment
for the
Data Analysis Support Laboratory

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: November 14, 2024

(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.)

This Privacy Impact Assessment (PIA) updates the Data Analysis Support Laboratory (DASL) PIA published in September 2018. To remain at the forefront of operational technology, the FBI continuously tests and develops new technology to support its law enforcement and national security missions. DASL, managed by the Criminal Justice Information Division (CJIS), provides the FBI with a secure information technology (IT) environment to research and develop new or improved systems, equipment, products, and devices. DASL maintains a collection of unclassified person-centric biometric and biographic information from various sources, such as internal FBI systems, research data collected pursuant to government oversight, and research data collected in coordination with academic partners. The data within DASL is used for the sole purpose of research, development, testing, and evaluation.

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.

DASL consists of a virtual networked environment, which is accessed from physical on-site locations. The physical environment includes the physical hardware (e.g., computers, servers, memory, storage) in DASL. There are four physical locations of DASL: one is located inside the CJIS Division with the other three managed by an FBI contractor, qualifying as federally funded research and development centers (FFRDC)[1]. The virtual network runs in an approved FBI cloud environment. These approved cloud environments are not yet active, but are expected to be on-line in the future, when they will contain relevant datasets, unique software applications, databases, computers, and storage to support the research, development, testing, and evaluation projects.

DASL uses carefully selected data sets to perform testing and evaluation of various identity and biometric technologies. Most of the testing data within DASL has been obtained from the Next Generation Identification (NGI) System. The NGI System (also managed by the CJIS Division) serves as the FBI's national biometrics and criminal history repository. The biometrics within the NGI System include ten-print fingerprints, face images, latent prints, and iris images submitted by criminal justice, national security, and other authorized government partners. The NGI System has separate, published PIAs for its various biometric modalities and services. Testing biometric matching algorithms and other biometric capabilities within DASL is essential for ensuring the most accurate identity data and the best functioning of the NGI System. Biometrics are tested in DASL for both

[1] *See* 48 CFR 35.107.

future operational implementation and for improvements in current processes. For example, the accuracy of iris images as an identification biometric was researched for several years before becoming an operational biometric in the NGI System. For biometric research projects, additional personally identifiable information (PII) associated with the biometric is typically removed. Evaluation in DASL is performed on the minimal amount of PII needed to accomplish the goal of the research project.

In addition to the NGI System, DASL uses biographic identity data from other CJIS-managed systems, such as the National Crime Information Center (NCIC), Uniform Crime Reporting (UCR), and the National Data Exchange (N-DEx). All CJIS systems with data used for internal research purposes have separate, published PIAs. FBI data scientists and analysts use the systems' information to discover data correlation, automation solutions, and potential trends. Analysis is often performed at the request of the relevant FBI program office or system owner. Use of realistic test data from operational environments is critical to validating the effectiveness of new and current technology. Findings from this research can improve situational awareness, support strategic decision-making, identify needs for system enhancements, and increase operational effectiveness.

Research may be performed across systems to produce analysis for FBI users of the information. For example, biometric identity data within the NGI System may be compared to biographic identity data within NCIC or N-DEx to assist with locating missing persons or persons with active warrants. Although not a significant part of DASL at this time, data from other FBI systems, including data collected by the FBI from other federal partners (e.g., Department of Defense, Department of Homeland Security), may be used for research and development projects. Whenever data from one FBI system is transferred into another FBI system, such as UCR data being placed in DASL, the FBI conducts an internal review assessing the mission need, the authority, the privacy risks, the dissemination controls, and other factors before approving the transfer or duplication of data.

Another source of information within DASL is biometric data and other PII obtained pursuant to the approval and oversight of the FBI's Institutional Review Board[2] (IRB). Approval by the IRB places significant requirements on the collection and use of personal data in DASL. IRB oversight includes ensuring that participants are fully informed of the parameters of the research project, any risks associated with the project, how their information will be used and protected by the FBI, how long their information will be retained, and how they may withdraw from the research. To the extent the data in an IRB approved research project is collected directly from the individual, data subjects must provide voluntary and informed consent. [In the event any personal data in an approved research project are obtained from criminal justice sources, consent is not obtained or required.] After initial approval, the IRB conducts ongoing oversight of the research project, including an annual review. An example of IRB-obtained data in DASL is the ongoing collection of biometrics from sets of identical twins. The multi-year dataset of identical twins' biometrics in DASL enables the FBI to conduct various biometric algorithm evaluations. Tests conducted using this data confirmed that fingerprints and iris biometrics are truly unique.

DASL contains research data obtained via formal agreements and participation in academic consortiums with colleges and universities. Typically, this research is also approved by the FBI's IRB

[2] The FBI's Institutional Review Board is charged with the protection of human subjects during research activities, including the collection of biometric information and other PII. *See* 28 CFR Part 44.

and/or the IRB of the other participating institution. Use of IRB/academic collected data often enables test and evaluation activities of niche populations or unique circumstances that would not otherwise be possible. In many circumstances, the academic consortiums with colleges and universities will make their datasets publicly available to any group within the research or industrial community to promote overall technology advancement. Finally, DASL accepts data from private vendors for the limited purpose of testing and certifying fingerprint collection devices. The CJIS Division maintains a public list of certified devices that meet the technical and quality requirements for fingerprint submission to the NGI System[3].

Regardless of the biometrics or other PII being used, the information is only stored in DASL for as long as necessary to complete the specific test and evaluation effort. Once the research is completed, the datasets will be removed. The length of time that the data remains in DASL varies depending on the research needs. Some data, such as photos from the NGI System for face recognition testing, will remain in DASL for a few years while other data may only remain for a few months.

The biometrics and other PII are not shared outside of the DASL environment except when the FBI shares sanitized—that is, pseudonymized--biometric data from the NGI System with the National Institute of Standards and Technology (NIST)[4]. The FBI has a long-standing relationship and interagency agreement with NIST for the international benchmarking of biometric algorithm accuracy. In accordance with this agreement, the FBI securely shares biometric data such as fingerprints, face images, and iris images with NIST to support accuracy testing. Prior to sharing this biometric data, the FBI removes unnecessary PII such as names and dates of birth. This process renders the biometric data pseudonymized; of course, biometric data by its nature cannot be completely anonymized. If necessary for the research, some demographic information such as age, race, and sex may be provided to NIST.

Aside from the datasets used for the test and evaluation efforts, the other information maintained in DASL consists primarily of test results, analytical findings, or reports. The results generated within DASL are often shared within the FBI and with external law enforcement partners. This information sharing provides accuracy findings or analytical trends that directly support criminal justice or national security operations. DASL returns data to private vendors limited to the certification process of each vendor's fingerprint collection device.

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	28 U.S.C. §§ 534, 534; 34 U.S.C. §10211(a)(2)
Executive Order	
Federal regulation	28 CFR 0.85

[3] *See* https://fbibiospecs.fbi.gov
[4] NIST, part of the Department of Commerce, is one of the nation's oldest physical science laboratories. Its core competencies include measurement science, rigorous traceability, and development and use of standards.

Agreement, memorandum of understanding, or other documented arrangement	
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, D	
Date of birth or age	X	A, B, C, D	
Place of birth	X	A, B, C, D	
Gender	X	A, B. C, D	
Race, ethnicity, or citizenship	X	A, B, C, D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	
Tax Identification Number (TIN)			
Driver's license	X	A, B, C, D	
Alien registration number	X	A, B, C, D	
Passport number			
Mother's maiden name			
Vehicle identifiers	X	A, B, C, D	
Personal mailing address	X	A, B, C, D	
Personal e-mail address	X	A, B, C, D	
Personal phone number	X	A, B, C, D	
Medical records number			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
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	X	A, B, C, D	
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	
Juvenile criminal records information	X	A, B, C, D	As permitted by federal/state laws
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**	X	A, B, C, D	

(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
- **Video containing biometric data**	X	A, B, C, D	
- **Fingerprints**	X	A, B, C, D	
- **Palm prints**	X	A, B, C, D	
- **Iris image**	X	A, B, C, D	
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, D	
- **Scars, marks, tattoos**	X	A, B, C, D	
- **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**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):			

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

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	
Phone		Email			
Other (specify): Information is collected directly from the person pursuant to IRB/academic research projects.					

Government sources:					
Within the Component	X	Other DOJ Components		Other federal entities	

Government sources:					
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): DASL does not collect information directly from federal, state, local, tribal or foreign governments; however, the NGI System and other CJIS systems contain criminal justice and national security biometrics and biographic data submitted by those entities.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify): Information is collected from members of the public pursuant to IRB/academic research projects. Information collection from the private sector is limited to certified fingerprint device vendors.					

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			Manual secure electronic transmission in support of FBI mission needs.
DOJ Components	X			Manual secure electronic transmission; only evaluation or analysis results.
Federal entities	X			Manual secure electronic transmission; only consist of evaluation or analysis results except for sanitized biometrics shared with NIST.
State, local, tribal gov't entities	X			Manual secure electronic transmission; only evaluation or analysis results.

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.**
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector	X			Manual secure electronic transmission; only data related to fingerprint device certification.
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.

The biometrics maintained within the NGI System may be used for FBI research and development purposes in accordance with applicable federal law and regulations. As discussed above, the FBI has a longstanding relationship with NIST to perform biometric testing. When the FBI provides pseudomized personal data to NIST, it is subject to strict security and use protections pursuant to an interagency agreement between the two agencies. Additional protections are delineated in "Government Furnished Information" letters which the FBI provides to NIST regarding specific research projects and data sets. Any biometrics used for research and development are sent without other associated PII; however, some non-unique biographic information may accompany the biometrics if required by the specific research activity. The data is encrypted in accordance with Federal Information Processing Standards 140-2 requirements prior to release. The data is stored in FBI laboratories which have received an authority to operate in accordance with FBI security policy and the Federal Information Security Modernization Act. In addition, only those with documented authorization and a true need-to-know are granted access to the data. No biometrics are 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.

All biometrics and associated PII submitted to DASL via an IRB or academic research collection are

provided voluntarily with the individual's notice and consent. The IRB regulations mandate numerous requirements to ensure that an individual's consent is knowing and voluntary. To the extent that the data is obtained from criminal justice sources, individualized consent is not obtained. The FBI has exempted itself from the requirement of 552a(e)(3) for the criminal and national security records maintained in the NGI System and other CJIS systems. The NGI System's SORN provides general notice that biometrics maintained in the system may be used for research and development. The most current version may be found at 84 Fed. Reg. 54,182 (October 9, 2019). This PIA also provides general notice that biometric and identity datasets in DASL derived from criminal justice data sets will be used for testing, evaluation, research, and development.

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.

For the IRB and academic research collections, participation is fully voluntary and the individuals are advised of the specific uses of their information. Data obtained from criminal justice sources does not involve the same protections. A person under investigation, arrest, or incarceration ordinarily has no opportunity to refuse the collection of biometrics or other identifying information. While federal agency criminal or national security uses of the information in the NGI System typically lack consent at the collection stage, they still must comply with other requirements in applicable law, including the Privacy Act.

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.

For personal data from the IRB and academic research collections, individuals have the right to cease participation in the research study at any time and are informed of how to request removal of their information from the research dataset. The IRB regulations require that these safeguards be in place for all approved research studies.

With respect to criminal justice data, Title 28 CFR part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act; and 28 CFR part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files pursuant to the Privacy Act. Title 28 CFR 16.30-16.34 establish specific procedures for an individual to obtain a copy of his or her criminal history record from the NGI System for review and correction. Note, however, that more for most of the records in the NGI and other CJS systems, the FBI maintains exemptions from access and amendment provisions of the Privacy Act. Other protections of the Privacy Act, including the protections for the confidentiality of records about individuals, are not subject to exemption under the Act.

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):** The ATO was issued in September 2023 and expires in September 2024. . **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:** No POAMs related to privacy controls.
	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	**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:** DASL has been assigned security categories as follows: Confidentiality – Moderate; Integrity – Low; and Availability – Low. The system has been assigned the confidentiality value of moderate because all of the information is unclassified and is not considered an official system of record, but often is composed of data collected in connection with law enforcement activity. Integrity and Availability were given an assignment of low because any data which resides in DASL will be used for research and development purposes only.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The ATO requires constant monitoring and logging functions to document all IT interactions within DASL. These measures have been in place and are being utilized.
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 ATO requires system administrators to audit the logs and system access records for compliance with security measures weekly.
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:**

	General information security training. Training specific to the system for authorized users within the FBI. Training specific to the system for authorized FFRDC users.

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?

DASL was specifically configured to reduce risks associated with unauthorized access. A technical control incorporated into DASL ensures that DASL does not have connectivity to the Internet. FBI approved and encrypted external storage devices are leveraged to securely transfer data from its original collection or system into DASL. This configuration requires appropriate steps such as security updates and software dependencies, appropriately scanned and evaluated for vulnerabilities, before the data is transferred to DASL. Data in transit is encrypted using Transport Layer Security Federal Information Processing Standard 140-2 encryption.

Only a limited number of FBI and authorized contractor personnel have access to the information in DASL. Role based access controls are employed to further limit access to the datasets based on work assignments. Access by FBI and contractor personnel to specific FBI applications and datasets are determined at the application and dataset level. Audit logs and user login identifiers are collected, maintained, and reviewed by the FBI.

All personnel who have access to DASL are required to take training specific to the function they will be performing. For example, general DASL user training is required for those granted physical and logical access to the system and DASL system administrators take more advanced training. These training courses highlight security and privacy requirements that all must adhere to while working within DASL.

DASL follows all FBI security policies and protocols regarding system security including (1) security measures that log all user activity while working in DASL, (2) ensuring both physical and logical access control techniques are utilized by all DASL users, and (3) utilizing automatic lockout if user inactivity exceeds a specified time frame.

Security controls for DASL are implemented to protect data that is shared, migrated, stored, used, and destroyed by the system. The FBI mandates the use and compliance with security controls listed in NIST SP 800-53 to address general protections of data and systems. The items listed below are some of the NIST SP 800-53 controls that help safeguard data stored in DASL.

- **Access Enforcement (AC-3)** – Account creation and logical access are managed according to the account management policy. Functional managers request/approve accounts according to this policy.
- **Least Privilege (AC-6)** – Role-based Access Control is strictly defined, enforced, and documented according to policy.
- **Audit Review, Analysis, and Reporting (AU-6)** – Automated mechanisms are in place to

detect, identify, and report suspicious activity which would then trigger supplemental manual processes for review and analysis.

- **Identification and Authentication (Organization Users) (IA-2)** – DASL uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
- **Media Access (MP-2)** – Access is restricted to all types of digital and/or non-digital media containing information not cleared for public release to authorized personnel in accordance with FBI Policy Directive 0247D, Removable Electronic Storage Media Protection, and FBI Policy Directive Draft for Mobile Devices.
- **Protection of Information at Rest (SC-28)** – Mechanisms are in place to ensure DASL protects the confidentiality and integrity of all information not cleared for public release.

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.)

Information is deleted from DASL after the conclusion of the relevant research project, when the data is no longer useful to support a certain research project, or when directed by the IRB. The data placed into DASL from IRB approved research projects generally has very limited retention, as the FBI IRB requires destruction of identifying data within a few years. The original identity records are maintained according to their respective system of records retention schedules. For the NGI System, the National Archives and Records Administration approved the destruction of fingerprint cards and associated information, including other biometrics, when criminal and civil subjects attain 110 years of age or seven years after notification of death with biometric confirmation.

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:

The Next Generation Identification System, 81 Fed. Reg. 27284 (May 5, 2016), amended by 82 Fed. Reg. 24156 (May 25, 2017) and 84 Fed. Reg. 54182 (October 9, 2019).

The FBI Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998), as amended by 66 Fed. Reg. 8425 (Jan. 31, 2001), as amended by 66 Fed. Reg. 17200 (Mar. 29, 2001), and 82 Fed. Reg. 24147 (May 25, 2017).

The FBI is currently drafting a SORN specific to research and development records.

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.***

Most data maintained in DASL originates from the FBI's performance of its law enforcement and national security responsibilities and is evaluated within DASL for the sole purpose of furthering those same responsibilities. In other words, DASL data consists of copies of internal operational data originally collected pursuant to the FBI's legal authorities. The majority of biometric and identity information used for testing purposes in DASL is obtained from the NGI System, the FBI's biometric and criminal history record system. The NGI System maintains biometrics such as fingerprints, palm prints, and photos of individuals who have been arrested or otherwise legally detained or processed in the criminal justice system. Only the identity data necessary for a specific research project is transferred to DASL. For example, a project to develop an improved latent print algorithm would not include the transfer of photos from the NGI System to DASL. DASL may also use identity data from other FBI systems, such as NCIC, the FBI's national law enforcement system. In these instances, DASL is assessing information that has been previously authorized for collection to improve the FBI's systems and processes.

The federal systems from which DASL obtains personal information are subject to a range of legal protections such as the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Modernization Act, and the Federal Records Act, as well as a range of internal controls and audits required by the Office of Management and Budget and FBI policy. Subject to these protections, the records in these systems may be shared with government employees and contractors for testing and evaluation performed in accordance with statutory and regulatory requirements. Access to data within DASL is limited to only those FBI or contractor personnel assigned to a specific research project. Once the research effort is complete and the data is no longer needed, it is removed from DASL.

The source of data considered for each research project is evaluated to minimize privacy risks. For example, if a certain testing and evaluation effort requires only the use of information already in FBI possession, then data from other sources will not be transferred to DASL. The biometric or identity information is rarely shared outside of DASL. However, if data is shared outside of DASL, action is taken to remove all unnecessary PII prior to doing so. For example, if biometric data is shared with NIST to support biometric algorithm testing, all biographic PII is removed from the dataset prior to sharing. This action combined with FBI encrypted transmission requirements and security requirements built into the interagency agreement with NIST are strong mitigations which reduce

privacy related risks.

In some instances, DASL uses information collected from FBI research projects that have been presented to and approved by the FBI's IRB. The IRB reviews and places limitations on all human subject research conducted by the FBI, including cooperative research projects with academic or other government partners. In compliance with the Protection of Human Subjects regulations, the IRB evaluates the risk to the subjects, ensures that informed consent was obtained from the subjects, and requires that the subjects' records are destroyed within a set time period[5]. When this research information is transferred to DASL, it remains subject to these protections.

The FBI has entered into formal agreements, such as cooperative agreements or memoranda of understanding, with the research components of academic institutions. Similar to the FBI's IRB requirements, an academic IRB must have reviewed and approved the research project and issued stipulations for the use of the information before DASL may accept it. When this research information is transferred to DASL, it remains subject to these protections. Collection of various sets of data to be used for test and evaluation purposes is traditional practice within the scientific community. The IRB/academic data collected for use in DASL is specifically tailored to current operational technology needs of the FBI. DASL does not retain biometric or other identity data from any public, private, or other source beyond the federal systems and IRB/academic approved research projects described above.

[5] *See* 28 C.F.R. 46.101-46.124