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 A. Winn, Acting Chief Privacy and Civil Liberties Officer, U.S. Department of Justice

Date approved: September 30, 2018

(May 2015 DOJ PIA Form/FBI revision August 1, 2017)

EXECUTIVE SUMMARY

The FBI's Data Analysis Support Laboratory (DASL) enables testing and evaluation (T&E) of identity and biometric technology in a secure environment. DASL provides the capability to evaluate Commercial Off-the-Shelf (COTS), Open Source, Government Off-the-Shelf (GOTS), and project-developed software. Biometric and identity information from FBI systems and government and academic partners are placed in DASL for the sole purpose of T&E in support of FBI initiatives and operational capabilities.

Section 1: Description of the Information System

(a) the purpose that the records and/or system are designed to serve:

DASL assists the FBI with the development of improved operational technology. DASL uses carefully selected data sets to perform T&E of various identity and biometric technologies. For example, biometric data from FBI systems such as Next Generation Identitification (NGI)[1] is placed into DASL to test and evaluate new biometric matching algorithms for future operational implementation.

(b) the way the system operates to achieve the purpose(s):

DASL is an FBI-owned and managed testing system residing on a closed network with the necessary software, computational capability, and storage volume needed to support FBI T&E requirements. This configuration provides an environment where new identity and biometric technology may be installed and evaluated quickly and effectively. For example, DASL has the capacity and infrastructure to run biometric matching software in a test environment with NGI data to identify performance characteristics such as accuracy. This capability enables the FBI to evaluate new technology in a safe environment in the most economical way possible.

(c) the type of information collected, maintained, used, or disseminated by the system:

Only the information required to complete a specific T&E effort is stored in DASL and that information will vary depending on the project. Currently, the datasets in DASL are largely composed of biometrics (i.e. photos and fingerprints) from NGI and from the FBI's federal and academic partners. The biometrics residing in DASL have been anonymized to the extent possible. No biographic information (e.g. name, date of birth) is associated with the biometrics.

[1] *See* Next Generation Identification System of Records Notice (SORN), 81 Fed.Reg 29,284 (May 5, 2016)

However, in some instances, the FBI may need to test biographic data, such as when developing improved name search algorithms for its systems, using biographic information. The reports from the T&E projects, which are retained, generally avoid including specific biometric or biographic information, as opposed to statistical analyses.

When the T&E effort does not require actual identity data, DASL creates synthetic data sets of identity information—that is, artificial data sets developed in a laboratory environment. Synthetic data do not correspond and therefore are not linkable to any actual individuals. For example, synthetic data sets are used if the goal of a particular T&E effort is to assess performance of alpha-numeric search algorithms, when the use of actual identity data is not needed.

(d) Who has access to information in the system:

Only FBI personnel or FFRDC personnel with a valid need-to-know and who are assigned duties pursuant to an active FBI contract have access to DASL. Biometric and biographic data in DASL are not disseminated outside of the system and are available only to the FBI and its contractors. T&E reports and synthetic data may be disseminated outside of DASL.

(e) how information in the system is retrieved by the user:

DASL users are assigned a unique username and password for access to DASL hardware and software. Internal security controls limit logical access to only those files, folders and data necessary for each individual user. This process allows DASL users to access information needed to complete their projects, while maintaining 'need to know' compliance at the same time.

(f) how information is transmitted to and from the system:

Identity and biometric data sets are transmitted to and from DASL using an encrypted storage media in accordance with FBI security policy. Encrypted storage media is also used when transferring T&E results or synthetic data sets to and from DASL.

(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects):

DASL is a stand-alone, non-operational testing environment with no connectivity to other systems.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):					

General personal data					
Name	x	Date of birth	x	Religion	
Maiden name	x	Place of birth	x	Financial info	
Alias	x	Home address		Medical information	
Gender	x	Telephone number		Military service	
Age	x	Email address		Physical characteristics	
Race/ethnicity	x	Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints	x	Photos	x	DNA profiles	
Palm prints	x	Scars, marks, tattoos	x	Retina/iris scans	x
Voice recording/signatures	x	Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify)					

System admin/audit data					
User ID	x	Date/time of access	x	ID files accessed	x
IP address		Queries run		Contents of files	
Other system/audit data (specify):					

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	
Telephone		Email			
Other (specify):					

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

Non-government sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (specify):	Academic Institutions				

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The majority of the biometric information used for T&E purposes in DASL is obtained from NGI, the FBI's biometric and criminal history record system. NGI maintains biometrics such as fingerprints, palmprints, and photos, of individuals who have been arrested or otherwise legally detained or processed in the criminal justice system. DASL may also use identity data from other FBI systems, such as the National Crime Information Center (NCIC), the FBI's national law enforcement system, or from other federal systems, such as the Department of Defense's biometric system. The systems from which DASL obtains personal information, of course, are themselves subject to a range of legal protections such as the Privacy Act, the e-Government Act, the FISMA and the Federal

Records Act; as well as a range of internal controls and audits required by OMB and agency policy. Subject to these protections, the records in these systems may be shared with government employees, contractors, and others for research performed in accordance with statutory and regulatory requirements, including Parts 22 and 46 of Title 28 of the Code of Federal Regulations. When information from these systems is transferred to DASL, it remains subject to these protections [2]

In some instances, DASL also uses information collected from FBI research projects that have been presented to and approved by the FBI's Institutional Review Board (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.[3] When this information is transferred to DASL, it remains subject to these protections.

Finally, 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 information is transferred to DASL, it remains subject to these protections.

DASL does not maintain identity or biometric data from any public, private, or other source beyond the federal systems of records and IRB-approved research projects described above.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities		For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
x	Other (specify): Testing and Evaluation		

[2] *See, e.g.,* Next Generation Identification SORN, Routine Use "W".
[3] See 28 C.F.R. 46.101-46.124.

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The information in DASL is used to perform T&E of identity and biometric technology. For example, testing the accuracy of fingerprint match algorithms requires use of fingerprint images. To evaluate algorithm performance, a gallery of fingerprint images is needed along with a second, and often smaller, set of fingerprint images to be used as search probes. Match accuracy is calculated by examining whether or not the algorithm correctly determines if the probe fingerprint image is a match to a fingerprint image in the gallery. Depending on the T&E need, these types of tests produce meaningful statistical conclusions for identity and biometric technology performance. These results are used to establish benchmarks for the technology available on the market. As the FBI and the U.S. Government continue to expand their use of biometrics, the T&E performed in DASL insures that the FBI has available to it to the most advanced and effective versions of these technologies, which helps to protect against the misidentification of individuals by the FBI's operational systems.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
x	Statute	28 U.S.C. §§ 533, 534.
	Executive Order	
	Federal Regulation	28 CFR 0.85, 28 C.F.R.46.101-46.124.
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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.)

Most information is deleted from DASL after the conclusion of the relevant T&E project or when the data is no longer useful to support a T&E effort, except as required by the Federal Records Act, in which case the data placed into DASL is subject to the respective records retention schedules for the systems from which the data was obtained. For NGI, 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. The data placed into DASL from IRB-approved research projects generally has a very limited retention schedule, as the FBI IRB requires destruction of

identifying data within a few years.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

Several mitigation methods have been employed to protect against threats to privacy regarding data stored in DASL. DASL is a standalone system with no connectivity to other FBI systems or the internet. This configuration greatly reduces the risk of an external entity gaining unauthorized access to DASL information. Furthermore, both physical and logical access control measures have been implemented to protect against unauthorized DASL access. Only FBI employees and FFRDC staff with a valid 'need to know' are granted access to DASL information. All personnel granted access to DASL information hold security clearances and receive annual privacy and information security training. A security assessment of DASL hardware and software has been completed and additional security controls have been implemented to protect against unauthorized DASL access. For example, DASL user activity is logged and can be audited at any point to ensure security protocols are being followed.

PII Confidentiality Risk Level:

☐ **Low** ☐ **Moderate** ☑ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** ☑ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII.
X	Separation of Duties: users of de-identified PII data are not also in roles that permit them to access the information needed to re-identify the records.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.

X	Remote Access: remote access is prohibited or limited to encrypted communication channels.
X	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching PII access authorizations to access restrictions, such as contractual/MOU/MOA requirements.
X	Access Control for Mobile Devices: access to PII is prohibited on mobile devices or limited so that data can only be accessed on mobile devices that are properly secured and regularly scanned for malware.

Audit controls

X	Auditable Events: access to PII is audited for unauthorized access.
X	Audit Review, Analysis, and Reporting: audit records are regularly reviewed for inappropriate or unusual activity affecting PII; such activity is investigated and reported; and responsive action and appropriate mitigation is taken.

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified and authenticated before accessing PII; remote access requires 2-factor authentication and 15-minute "time-out" functionality.

Media controls

X	Media Access: access to system media containing PII (CDs, USB flash drives, backup tapes) is restricted.
X	Media Marking: media containing PII is labeled with distribution/handling caveats.
X	Media Storage: media containing PII is securely stored.
X	Media Transport: media is encrypted or stored in a locked container during transport.
X	Media Sanitation: media is sanitized prior to re-use.

Data Confidentiality controls

X	Transmission Confidentiality: DASL is a standalone T&E environment, information stored within DASL is not transmitted outside DASL; information can only be added to or taken out of DASL manually by authorized DASL users leveraging encrypted storage media (**Required if the system meets the NIST 800-59 definition of a National Security System**.)
X	Protection of Information at Rest: DASL is a standalone T&E environment with no internet connectivity, DASL spaces employ strict physical and logical access controls to ensure only authorized users with a valid need-to-know have access to DASL information (**Required if the system meets the NIST 800-59 definition of a National Security System**.)

Information System Monitoring

X	Information System Monitoring: network boundaries are automatically monitored for unusual or suspicious transfers or events

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Only T&E reports and synthetic data are shared beyond the users of DASL. The recipients marked below would not ordinarily receive biometric and identity data from DASL; they would only receive conclusions from a specific T&E effort. If a report needed to use a specific individual's biometric as an example, reasonable efforts are used to maintain the anonymity of the biometric information. Reports summarizing T&E results may include information regarding how a test was conducted, metrics used for evaluation, and conclusions made. Also, synthetic data may be disseminated outside of DASL. For certain T&E efforts, synthetic data may be provided to vendors for product improvement prior to official testing activities.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	x			
DOJ components	x			
Federal entities	x			
State, local, tribal gov't entities	x			
Public				
Private sector	x			
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

As explained above, almost no personally identifiabile information (PII) is disseminated from

DASL. The biometric and identity data in DASL is available to only those FBI employees and contractors who are assigned to work on the T&E projects in DASL. These employees and contractors must have a valid need to know the information. DASL users are assigned a unique username and password for access to DASL hardware and software. Internal security controls limit logical access to only those files, folders and data necessary for each individual user. FBI management has implemented safeguards for PII protection such as standard operating procedure and policy requirements, education, training, and awareness. These safeguards are combined with relevant and related IT security controls as part of a comprehensive privacy program. Users are subject to Annual Security Awareness training that includes how to identify and protect PII. The required annual training refresher also serves to reinforce policies and procedures, such as access rules, retention schedules and incident response.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

x	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
x	Yes, notice is provided by other means.	Specify how: For IRB research, all participants receive notice that their information will be used for T&E purposes.
x	No, notice is not provided.	Specify why not: For NGI and other federal systems, the information is collected pursuant to authorized criminal investigations.

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

x	Yes, individuals have the opportunity to decline to provide information.	Specify how: For IRB research, participation is voluntary and individuals must provide an informed consent regarding the use of their information.
x	No, individuals do not have the opportunity to decline to provide information.	Specify why not: For NGI and other federal systems, the information is collected pursuant to authorized criminal investigations.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

x	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: For IRB research, participation is voluntary and individuals must provide an informed consent regarding the use of their informaion.
x	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: For NGI and other federal systems, the information is collected pursuant to authorized criminal investigations.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

A person under arrest or the subject of a criminal or national security investigation generally has no opportunity or right to refuse the collection of biometrics or identity information. Consequently, the data retained in DASL from NGI and other federal systems was not obtained with individual notice and consent. However, information about the collection, maintenance, or use of biometrics and identity information for T&E purposes are communicated in general notices to the public via the FBI's published SORNs, this PIA and other Privacy Act notices. For biometrics and identity information collected via IRB-approved research, full notice and informed consent are required by the federal regulations. Consent forms must be signed by each volunteer to document full understanding of why his/her information is being collected and how it will be used. If an individual prefers not to consent for any reason during the research project, his/her biometrics will not be collected.

Section 6: Information Security

6.1 Indicate all that apply.

x	A security risk assessment has been conducted. A security risk assessment was completed in September 2017.
x	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Security controls have been documented in the Security Requirement Traceability Matrix (STRM).

x	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Information safeguarding activities and their frequency are outlined in the DASL System Security Plan (SSP)	
x	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: ATO is pending.	
x	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information:	
x	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
x	The following training is required for authorized users to access or receive information in the system:	
	x	General information security training
	x	Training specific to the system for authorized users within the Department.
	x	Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

Privacy-specific safeguards have been implemented in DASL as controls for protecting stored data. DASL is in compliance with 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 processed, stored, or transmitted 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 are assessed to 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 (RBAC) is strictly defined, enforced and documented according to policy.
- **Audit Review, Analysis, and Reporting (AU-6)** - Automated mechanisms are in place to detect and identify and report suspicious activity which would then trigger supplemental manual processes for review and analysis.

- **Identification and Authentication (Organizational Users) (IA-2)** – DASL uniquely identifies and authenticates organizational users (or processes acting on behalf of organtizational 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.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: FBI Central Records System, 63 Fed.Reg. 8659,671 (February 2, 1998).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information in DASL is retrieved by biometric matching algorithms that identify persons based on their biometrics. Information may also be retrieved with biographic information if necessary and if available. DASL provides the highest levels of data protection possible and does not operate differently with regard to citizenship status.