Federal Bureau of Investigation

Privacy Impact Assessment
for the
BRAG Database

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: [November 17, 2020]

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

EXECUTIVE SUMMARY

This Privacy Impact Assessment (PIA) describes how the Federal Bureau of Investigation (FBI) performs background investigations of those persons seeking employment that require access to biological agents and toxins. Pursuant to federal statute, the FBI must collect information from these individuals, perform research, and appropriately share relevant findings with authorized agencies. This information is maintained in the CJIS Division's Bioterrorism Risk Assessment Group (BRAG) Database. This PIA addresses the privacy risks and mitigations regarding collecting personally identifiable information (PII) of individuals submitted to the FBI for this authorized purpose.

Section 1: Description of the Information System

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

Section 201 of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act), Public Law 107-188, which amends the Public Service Health Act, codified at 42 U.S.C. § 262a, restricts individual access to certain dangerous biological agents and toxins. Pursuant to the Bioterrorism Act, the Secretaries of the Departments of Agriculture (USDA) and the Department of Health and Human Services (HHS), in consultation with the Attorney General, are responsible for establishing appropriate safeguards and security requirements for individuals possessing, using, or transferring select biological agents and toxins. The USDA and HHS determine whether individuals have a legitimate need to handle or use biological agents by initiating security risk assessments (SRAs) that include assigning unique numeric identifiers to applicants and providing the Attorney General with the names and other identifying information of these applicants.

With the identifying information, the Attorney General is required to conduct searches of available databases and evaluate individuals under the Bioterrorism Act. The statute requires the Attorney General to "promptly use criminal, immigration, national security, and other electronic databases that are available to the Federal Government and are appropriate for such purpose" to conduct the SRAs. *See* 42 U.S.C. § 262a(e)(3)(A). The Attorney General delegated the duty to perform SRAs to the FBI's Criminal Justice Information Services (CJIS) Division's Bioterrorism Risk Assessment Group (BRAG). After BRAG conducts the SRA, it must promptly notify USDA or HHS whether any disqualifying information has been found. The BRAG Database maintains this federally required information.

The statute provides that individuals will be disqualified from possessing, using, or transferring select biological agents and toxins if the person meets any of the following criteria identified in 18 U.S.C. section 175b(d)(2) and 42 U.S.C. § 262a(e)(3)(B):

- an individual who has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year;
- an individual who is under indictment for a crime punishable by imprisonment for a term exceeding one year;

- a fugitive from justice;
- an unlawful user of any controlled substance (as defined in Section 102 of the Controlled Substances Act);
- an alien illegally or unlawfully in the United States;
- persons who have been adjudicated as a mental defective or committed to any mental institution;
- an alien (other than an alien lawfully admitted for permanent residence) who is a national of a country that the Secretary of State has determined repeatedly support acts of international terrorism;
- individuals who have been discharged from the Armed Services of the United States under dishonorable conditions;
- is a member of, acts for or on behalf of, or operates subject to the direction or control of a terrorist organization;
- is reasonably suspected by any federal law enforcement or intelligence agency of committing a crime of terrorism as set forth in Section 2332b(g)(5) of Title 18, United States Code;
- is reasonably suspected of knowing involvement with an organization that engages in domestic or international terrorism (as defined in Section 2331 of Title 18) or with any other organization that engages in intentional crimes of violence;
- is reasonably suspected of being an agent of a foreign power (as defined in Section 1801 of Title 50).

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

To fulfill the requirements of the Bioterrorism Act and to conduct the SRAs, BRAG obtains a Bioterrorism Preparedness Act: Entity/Individual Information Form (FD-961) from individuals applying for access to select agents and toxins. The information on the FD-961 is entered by the individual and the form may be sent to BRAG directly by the individual or by the sponsoring agency. The FD-961 may be mailed in hard copy or it may be emailed to BRAG. The FD-961 is emailed to BRAG's Law Enforcement Online (LEO) account, which is a secure, encrypted site.

BRAG enters the biographic information from the FD-961 into the BRAG Database, which is a restricted web application that features a server database as well as reporting services. The BRAG Database provides a centralized location for BRAG to maintain information on the individuals on whom it conducts SRAs. The database resides on CJIS Unet, which is a multi-purpose unclassified network that supports and provides access to various FBI systems, applications, and functions.

BRAG uses information from the FD-961 to conduct biographic searches of relevant databases to determine if the applicant is subject to any of the statutory disqualifiers. In particular, BRAG searches both classified and unclassified FBI systems to determine if an individual has prohibiting criminal history, is a fugitive from justice, is a known or suspected terrorist, or should otherwise be restricted under the Bioterrorism Act. BRAG also queries appropriate systems of other federal agencies to obtain relevant information, such as foreign intelligence, mental health, military service, and immigration status. These systems consist of those maintained by the Department of Homeland Security, the

Department of Defense, the Department of Veterans Affairs, and the Office of the Director of National Intelligence. BRAG maintains a law enforcement account to search Lexis/Nexis Accurint for additional biographic and disqualifying information. The FBI and federal systems searched by BRAG are covered by separate Privacy Impact Assessments and Privacy Act System of Records notices as necessary. Each system searched and any relevant information obtained from these systems is documented in the BRAG Database. BRAG may also enter notes and comments in the database regarding any findings.

Upon receipt of all responses from the various systems, BRAG performs the SRAs to determine whether the individual is a restricted person pursuant to the Bioterrorism Act. The determination is entered in the BRAG Database and BRAG also uploads the SRA to the restricted BRAG files in Sentinel, the FBI's classified case management system. The Sentinel file maintains the actual print-outs from the system searches and contains any relevant classified information. Only BRAG has access to the Sentinel files and others in the FBI must reach out to BRAG for additional information on any individual of interest. If an individual is found to be restricted, BRAG advises the appropriate FBI Division.

After completion of the SRA, BRAG forwards its recommendation via hard copy or encrypted email to the USDA and HHS and those agencies make the final determination as to whether an individual will be allowed to access select agents and toxins. BRAG provides only the name, date of birth, and decision in its recommendation. If the applicant is recommended to be disqualified, BRAG will provide the disqualifier to the USDA and HHS and, if requested, underlying derogatory information or investigative findings. Unless approval is terminated by the USDA or HHS, the SRA is valid for three years.

Each applicant must also send a set of ten-print fingerprints to BRAG that are collected on a hard copy FBI fingerprint card (FD-258). BRAG scans the fingerprints into the Next Generation Identification (NGI), the FBI's biometric and criminal history system. The fingerprints are queried against NGI to positively identify the applicant and to determine if he/she has a disqualifying criminal history. At the same time, the fingerprints are queried against the Department of Defense's Automated Biometric Identification System (ABIS) and the Department of Homeland Security's Automated Biometric Identification System (IDENT), via the interoperability rules between NGI, ABIS, and IDENT. The fingerprints are also queried against the Royal Canadian Mounted Police's Real Time Identification. Any additional biographic information, disqualifying criminal history, or other disqualifier found as a result of the fingerprint queries are documented in the BRAG database and Sentinel.

When entered into NGI, the applicant's fingerprints are also enrolled in the CJIS Division's Rap Back[1] service. The fingerprints are enrolled in Rap Back for an initial period of three years and are retained longer if an individual submits a renewal FD-961 to BRAG. The Rap Back enrollment permits BRAG to receive immediate notifications of criminal history events entered into NGI, such as a subsequent arrest or updates to existing criminal history records. Any criminal history information obtained from

[1] Rap Back has separate privacy documentation.

NGI regarding an individual is notated in the BRAG database. If the individual is found to have a disqualifier after being enrolled in Rap Back, the individual is removed from Rap Back upon notification to the FBI from the sponsoring agency. In addition to the biographic information collected on the FD-961, each applicant must attach a facial photo to the FD-961. BRAG scans these photos and stores them in the Civil Identity File in NGI. These photos are not searchable or available to any other users of NGI.

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

BRAG collects a significant amount of PII from applicants on the FD-961 in order to effectively and accurately complete the SRAs. The FD-961 requires name, date of birth, place of birth, address, Social Security number, driver's license number, email address, phone numbers, and other PII necessary to search for disqualifiers. As mentioned above, the applicants must also submit facial photos and fingerprints. BRAG does not maintain the FD-961 forms or fingerprint cards in hard copy. After the information is entered into the BRAG database, Sentinel, and /or NGI, the hard copies are destroyed. BRAG may collect and maintain additional PII in the BRAG Database from systems that were queried during the course of the SRA. The BRAG Database also contains unique identifying and transaction numbers that are linked to the individual applicant.

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

Only FBI employees assigned to BRAG and supporting information technology (IT) personnel have access to the BRAG Database. BRAG consists of a small team of personnel and when someone is no longer assigned to BRAG, management requests IT personnel to suspend that person's access to the Database. Audit logs reflecting who accesses the BRAG database and any changes made to the database are accessible only to database administrators (please see Sections 2.3 and 6.2 for more information about the auditing process). Although the USDA and HHS do not have direct access to the BRAG Database, they receive reports that contain information found in the database. These reports contain basic administrative data (e.g. the sponsoring agency's unique identifying number and relevant decision dates) and the names and dates of birth of the applicants. Information in the BRAG Database and Sentinel is shared within the FBI on a case-by-case basis if there is a "need to know" the information. The fingerprints and photos in NGI are not disseminated to anyone outside of the FBI.

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

The BRAG Database is located on CJIS Unet, which requires users to have a login ID and two factor authentication. The BRAG database uses an individual's CJIS Unet login for access. Users are granted access based on their roles (administrator, supervisor, or user) by individuals with the appropriate permissions to grant access. Information from the BRAG Database may be retrieved by an individual's biographic descriptors, a unique identifying number (UIN or DOJ number) assigned by USDA or HHS to each individual, or BRAG record number (the number assigned to the applicant when entered into the BRAG Database).

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

Currently, the information from the FD-961 is manually entered into the BRAG Database by BRAG employees; however, BRAG is seeking an IT solution to automatically populate the FD-961 into the Database. BRAG similarly enters notations, findings, and determinations into the BRAG Database regarding any information from the queried systems within the FBI and other federal agencies. Each BRAG employee must have an individual user account for each system queried because the BRAG Database has no electronic connection to these systems. Likewise, BRAG must manually upload information into NGI and Sentinel because these FBI systems have no electronic connection with the BRAG database.

The BRAG database includes an import feature which allows BRAG employees to import withdrawn reports from USDA and HHS. Withdrawn reports list all individuals who have been removed from the select agent program. BRAG employees can also export SRAs from the BRAG Database. Once exported, the BRAG employees save the SRA to restricted files in Sentinel. These import and export reports are not automated; they are typically formatted in an Excel spreadsheet. BRAG destroys the withdrawn reports once all SRAs in that report are removed. BRAG maintains all information regarding the SRAs, queried system results, and FD-961 information.

BRAG has access to the database used by USDA and HHS and enters the SRA expiration dates and received dates on a daily basis. If requested, BRAG may send a report containing the applicant's name, date of birth, unique identifying number, and the entity at which each applicant is working, along with the final decision from BRAG. If BRAG recommends that an applicant be restricted, BRAG also provides a letter, which is signed by the BRAG Supervisor. The letter is sent via encrypted email to the sponsoring agency and the original letter is mailed.

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

BRAG is a restricted web application that features a server database as well as reporting services. The application is deployed on CJIS Unet and is only accessible by users who have been approved by those in a Supervisor or Administrator role. While the application features import and export capabilities to other agencies and/or units these functions are done by BRAG users who possess the necessary roles to run these tasks. The application does not feature any automated connectivity to other projects or systems on CJIS Unet or any other system. As discussed above, BRAG queries internal FBI systems and the systems of other federal government agencies that are relevant to the determination of a federal disqualifier. BRAG users must log-in to each of these systems in order to manually review any necessary information.

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	X	Alien Registration	X	Financial account	
Taxpayer ID		Driver's license	X	Financial transaction	
Employee ID		Passport	X	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	X	Medical information	
Gender	X	Telephone number	X	Military service	
Age		Email address	X	Physical characteristics	X
Race/ethnicity	X	Education		Mother's maiden name	X
Other general personal data (specify):					

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

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		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	X	Contents of files	X
Other system/audit data (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	X	Online	
Telephone		Email	X		
Other (specify): The FD-961 and FD-258 are completed by the individual and sent to BRAG either by the individual or the sponsoring agency.					

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

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

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.)

BRAG collects only that information which has been deemed necessary to comply with its statutory mandate to conduct SRAs on applicants for access to dangerous biological agents and toxins. BRAG collects only that information necessary to establish identity and to research the statutory disqualifiers. Likewise, BRAG only searches those databases and systems that are most likely to provide disqualifying information. The biographic and biometric information is provided by the applicant; therefore, he/she has knowledge of all personal information being collected and has provided consent to its use for this purpose.

The collection and searching of the biographic and biometric information presents privacy risks that the personal information of individuals will be searched or disseminated for improper purposes, or that there will be improper access to or misuse of the information. This risk is significantly mitigated because the BRAG database is accessible to only BRAG and supporting IT personnel who have been approved by those in a Supervisor or Administrator role. The application does not feature any automated connectivity to other projects or systems on CJIS Unet. The BRAG information maintained in Sentinel and NGI is also only accessible to BRAG personnel, and those within the FBI who have requested access and have specific need to know

the information. Additionally, the risk that information will be searched for improper purposes is mitigated through auditing, which occurs from user logs, monitoring application use, and user activity. The audit review record is conducted at least every seven calendar days. See Section 6.2 for more information about the auditing process.

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): Pursuant to the Bioterrorism Act, the information is collected in order to conduct Security Risk Assessments on individuals who are applying for access to select agents and toxins.		

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.

As listed below, the FBI has statutory authority to collect biographic and biometric information from individuals applying for access to select agents and toxins. In compliance with this authority, the FBI uses the information collected to confirm the identity and conduct an SRA on individuals who are applying to the Select Agent Program. In so doing, the FBI helps to safeguard the American public from bioterrorism and other threats to public safety and national security. In the course of conducting an SRA, if BRAG discovers disqualifying information regarding an applicant, it will share this information internally with FBI agents for further criminal or national security investigation, as appropriate.

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	Public Law 107-188; 18 U.S.C. 175b, 28 USC 534, 42 USC 262a
	Executive Order	
X	Federal Regulation	7 CFR Part 331, 9 CFR Part 121, 42 CFR Part 73
	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.)

The National Archives and Records Administration (NARA) has approved the destruction of all documents related to the BRAG Database after fifty years of processing. Hard-copy information is destroyed immediately once electronically scanned into Sentinel, NGI, or the BRAG Database. The NARA-approved retention schedule for NGI has approved the destruction of fingerprints and associated information in NGI when the subjects attain 110 years of age, or seven years after notification of death with biometric confirmation.

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.]

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.
N/A	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.
N/A	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 reviewed at least weekly 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 30-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 (Be sure to also discuss in Section 1(f).)

X	Transmission Confidentiality: Information is encrypted prior to transmission or encrypted transmission is used. (**Required if the system meets the NIST 800-59 definition of a National Security System**.)
X	Protection of Information at Rest: Information stored on both primary and secondary storage devices (e.g., hard drive or backup tape) are encrypted. (**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.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X			
DOJ components				
Federal entities	X	X		
State, local, tribal gov't entities				
Public				
Private sector				
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 discussed above, the BRAG Database cannot be accessed by anyone other than BRAG and IT personnel with a need to access the database for the performance of their official duties. Information placed in Sentinel and NGI is also restricted to BRAG personnel and may be shared with others in the FBI on a case-by-case basis if there is a "need to know" the information. The fingerprints and photos in NGI are not disseminated to anyone outside of the FBI. The USDA and HHS do not have direct access to the BRAG Database and only receive individual recommendations and reports that have been created and approved by BRAG. This limited

access ensures that the PII of those applicants submitting an FD-961 is protected from unauthorized disclosure. In both instances, the USDA and HHS only receive the name and date of birth of applicants; information that both agencies already possess regarding the applicants. The recommendations and reports are sent via encrypted email and/or letter. The FBI provides this information to the USDA and HHS under its statutory obligation to perform SRAs, and the USDA and HHS are subject to federal regulations regarding their use of applicant information.[2] Further, the reports provided by BRAG to the USDA and HHS permit their databases to be compared with the BRAG database to ensure that the applicant lists are up-to-date and accurate.

User access to information within the BRAG Database is strictly controlled to protect privacy and reduce the risk of unauthorized access and disclosure. 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. Auditing occurs from user logs, monitoring application use, and user activity. The use of unique User IDs and strong passwords makes it difficult for a user to gain unapproved access or an inappropriately heightened level of access.

All privileged users are notified through warning banners and by signing the FBI Rules of Behavior that they are subject to periodic, random auditing of what searches they perform, when they perform the searches, and what data was accessed in all FBI information systems. This awareness is useful in discouraging unauthorized or non-work related searching and to provide awareness of data that has specific handling requirements or sensitivity.

In addition, the CJIS Information Assurance Unit (CIAU) is responsible for ensuring that mechanisms are in place to make certain that individuals are held accountable for implementing these controls adequately and that the controls are functioning as intended. Through the Security Assessment and Authorization (SAA) process and throughout the system lifecycle the CIAU and BRAG together provide oversight and accountability for the implementation of key controls, specifically those related to the information system security, Privacy Impact Assessments, and Privacy Act compliance.

The BRAG database is accredited as part of the CJIS UNet. As part of the SAA process, the CJIS UNet included a NIST 800-53 security control baseline at the HIGH/MODERATE/HIGH impact level of assurance (LOA). Access to the system is restricted as required by established security controls. Security controls are continually assessed during the application/system development life cycle for compliance and to ensure appropriate mitigation strategies have been implemented commensurate with the HIGH/MODERATE/HIGH impact LOA to protect the confidentiality, integrity and availability of data.

An Information Systems Security Officer (ISSO) and an Information Systems Security Engineer (ISSE) are responsible for ensuring the day to day implementation, continuous monitoring, and maintenance of the security configuration, practices, and procedures for CJIS Unet and the BRAG Database. The ISSO and ISSE assist the operational staff and program office to make certain that system security documentation is developed, maintained, reviewed and updated to reflect changes to the risk posture and privacy impact of the BRAG Database. If any system changes affect the confidentiality, integrity, or availability of the database, then additional or

[2] See https://www.selectagents.gov

different security controls may be required.

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: The Privacy Act statements on the FD-961 and the FD-258 explain the authority, purpose, and use of the information collected.
	No, notice is not provided.	Specify why not:

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: All information is provided voluntarily; however, if the applicant does not provide sufficient information for BRAG to complete an SRA, the applicant will not be granted access to select biological agents and toxins.
	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

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: All information is provided voluntarily for the specific purpose of applying for access to select biological agents and toxins. The applicant is advised of and authorizes this and other particular uses on the FD-961.
	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not:

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.

The individuals voluntarily provide PII to the FBI in order to apply for employment that requires access to dangerous biological agents and toxins. The Bioterrorism Act identifies the disqualifiers for such employment and provides notice of the FBI's authority to conduct an SRA by using the PII to research appropriate databases. The applicants receive individual notices regarding the authority, purpose, and use of their information on Privacy Act statements on the FD-961 and FD-258.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted. The most recent risk assessment was completed in July 2019.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Security Requirements Traceability Matrix (SRTM), National Institute of Standards and Technology (NIST) 800-53.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Active system administration and log reviews, automated monitoring, IBM Tivoli Identity Manager (ITIM), Enterprise Security Operations Center (ESOC). The information is secured in accordance with FISMA requirements.
X	Provide date of most recent Certification and Accreditation: The BRAG database is accredited as part of the CJIS UNet. CJIS UNet most recently received an ATO in April 2019.
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: Various commercial off-the-shelf products such as Rivest, Shamir, and Adelman (RSA) Security Analytics, Tripwire, and Digital Guardian assist in the monitoring and detection of malicious behavior.
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.
		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.]

The BRAG database is accredited as part of the CJIS UNet system. CJIS UNet implements privacy-specific safeguards as controls for protecting the confidentiality of PII. CJIS UNet is in compliance with all FBI security policies and protocols regarding system security, including (1) security countermeasures that hold all users accountable for their actions while on the computer system, (2) ensuring access control techniques are utilized, by the implementation of a management-approved Standard Operating Procedures guide for supervisors and staff, (3) utilizing security controls such as internal labeling of contents by classification labeling, and (4) utilizing automatic lockout if user inactivity exceeds a specified time frame.

Security controls for CJIS UNet are implemented to protect data that is processed, stored, or transmitted by the system. ISSOs and System Security Administrators continually review the security controls per the FBI Security Assessment and Authorization Policy Guide and also use the NIST special publication 800-53A, revision 4 for expanded definition and guidance. The ISSO is required to review security controls annually. Security Control Risk Assessment 5 focuses on assessing risk to reduce the risk of unauthorized access, use, and disclosure. The risk assessment is reviewed and updated at least annually. The security impact level for confidentiality in the CJIS UNet system is high and confidentiality is protected through acceptable security controls addressing boundary protection/external telecommunication, transmission confidentiality and integrity, and remote access/protection of confidentiality and integrity using encryption at rest and in transit.

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 the confidentiality of PII within CJIS UNet/BRAG Database.

- **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 using RSA Security Analytics, Tripwire, and Digital Guardian are in place to detect, identify, and report suspicious activity which would then trigger supplemental manual processes for review and analysis. Upon suspicion of malicious behavior, the CJIS-UNET ISSO is notified who, in turn, requests that the SSA review audit records to

determine if malicious activity has occurred. If necessary, the CJIS CSO is also notified.

- **Identification and Authentication (Organizational Users) (IA-2)** – CJIS UNet contains all accounts and individual identities. For internal privileged users, unique identities and accounts require authentication before access.
- **Media Access (MP-2) -** Removable media is restricted to privileged users, strictly enforced, monitored, and audited for unauthorized use. Privileged users are identified and vetted by the system, SSAs, SAs, and ISSOs.
- **Protection of Information at Rest (SC-28)** – CJIS UNet protects the confidentiality and integrity of information as the system is hosted within an accredited physical space with significant physical and logical protections on the Enterprise Storage System (ESS).

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 20, 1998); 66 Fed. Reg. 8425 (January 31, 2001); 66 Fed. Reg. 17200 (March 29, 2001); 72 Fed. Reg. 3410 (January 25, 2007) 82 Fed. Reg. 24151,156 (May 25, 2017).
	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 within the BRAG database may be retrieved by authorized FBI personnel via biographic identifiers and/or unique identifying numbers. Although the BRAG Database may contain citizenship data, no information is retrieved based on citizenship.