Federal Bureau of Investigation

Privacy Impact Assessment
for the
[Law Enforcement Enterprise Portal (LEEP)]

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

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

Date approved: [September 28, 2022]

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

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

The Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, Law Enforcement Enterprise Portal (LEEP), is a federated[1] gateway which securely connects law enforcement, criminal justice, national security, and public safety communities to systems via established secured connections. LEEP was developed by the FBI CJIS Division for secured electronic information sharing among federal, state, local, tribal, and territorial agencies. Select international entities and private sector individuals also access LEEP to share information with federal, state, local, tribal, and territorial agencies. The benefits of LEEP include a streamlined single sign-on[2] technology for users to access resources (*e.g.*, information sharing tools, reports, and training) on LEEP, and a user vetting solution which ensures only authenticated individuals have access to those resources. LEEP eliminates the need to register user identity information in multiple systems. This Privacy Impact Assessment addresses the privacy implications of LEEP collecting, maintaining, and sharing the personally identifiable information (PII) of its users and the mitigations in place to protect users' PII.

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.

The FBI CJIS Division Law Enforcement Support Section is charged with the development of LEEP. LEEP is designed to protect and manage access to systems by federal, state, local, tribal, and territorial criminal justice, national security, and public safety communities nationwide. Select international entities and private sector individuals also access LEEP to share information with federal, state, local, tribal, and territorial agencies. LEEP is a technical architecture-aligned solution that provides the FBI and other federal, state, local, tribal, and territorial agencies with the ability to identify, monitor, and manage individuals that access LEEP and FBI resources leveraging LEEP. This set of Enterprise Identity Management Services (EIMS) include enterprise Identity Credentialing

[1] "Federated" is a standard Information Technology (IT) industry term that refers to authenticated or trusted gateways/portals to networks for information sharing purposes. It implies a trusted community of users utilizing the same portal.

[2] "Single sign-on technology" is a standard industry term used to describe a technology that "employs a central authorization server to enable a user to authenticate one time in order to achieve access to multiple applications, machines, and domains operating with a variety of authentication mechanisms. . . . The central server establishes and maintains, as individual actions, the authorizations at each application, machine, or domain that the user is allowed to access." National Institute for Standards and Technology (NIST), Special Publication (SP) 800-36, Guide to Selecting Information Technology Security Products (Oct. 2003), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-36.pdf.

Access Management (eICAM), Security Identity Manager, Security Verify Access, Security Verify Governance, Federated Identity Manager, Portal Services, and Leap Forms, all operationally deployed as the LEEP system. This technical architecture combines to establish a centralized user interface and the establishment of hosted and federated Identity Providers (IdPs)[3] and Service Providers (SPs).[4] **Hosted IdPs** (e.g., LeepID IdP, National Instant Criminal Background Check System ECheck) are managed by the FBI and store user data within the LEEP system. **Federated IdPs** are external FBI partners who manage their user data and pass user attributes to LEEP for access at the user's request. Federated IdPs pass user attributes via Security Assertion Markup Language (SAML).[5] Any time the FBI onboards a new IdP or SP, the FBI provides the IdP or SP with a list of attributes (required or optional) accepted by LEEP and a definition for each attribute. The onboarding documents ensure all IdPs, SPs, and the FBI have a common understanding of what each attribute conveys.[6] The centralized user interface for LEEP is an internet and intranet web service which provides a centralized portal (**www.cjis.gov**). LEEP centralizes access to FBI criminal justice services along with other agencies' systems and services. Through LEEP, authorized users can access dozens of information systems including: cyber-crime investigative resources, situational awareness tools, nation-wide criminal justice records, national gang information, training tools, secure file sharing, national security and suspicious activity reporting data, geo-spatial tools, and crime statistics and police data reporting tools.

LEEP serves as the gateway for authorized users coming through an IdP who wish to use various SPs residing on the portal. Agencies may act as both IdPs and SPs. IdPs are responsible for vetting their users to ensure each user meets the requirements to access specific systems residing on LEEP. The IdPs are accountable for ensuring user information remains accurate and current. Some examples of current IdPs include various local and state police departments, the FBI, and the Department of Justice (DOJ).

Both IdPs and SPs must comply with the *LEEP Procedure and Operations Manual*, comply with the *CJIS Division Security Policy*, and have advanced authentication in place for their connection. FBI systems connected to LEEP are documented via an FBI Electronic Communication and connections to DOJ systems are documented with a Memorandum of Understanding (MOU). Non-FBI/DOJ agencies are required to sign an MOU with the FBI CJIS Division or have a current signed copy of the CJIS User Agreement on file with the FBI CJIS Division. The LEEP program office and the technical office reside at the CJIS Division to ensure technical, policy, and security compliance.

[3] An IdP is an organization/agency that creates, maintains, and manages identities of authorized users to access systems/services on LEEP.

[4] An SP is an organization/agency that creates, maintains, and manages a system/service or database on LEEP that is available to authorized users.

[5] SAML is a standardized markup language format used for exchanging authentication and authorization information. "Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials . . . enhancing the interoperability between disparate applications." See NIST SP 800-95, Guide to Secure Web Services (Aug. 2007), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf.

[6] For example, the "sworn law enforcement officer indicator" (SLEO) is used to assert that a user is a SLEO if all of the following conditions are true: the user is a full time employee of a state-recognized law enforcement agency; the user is authorized (has the authority) to make an arrest; and the user is certified by a State Certifying Authority (i.e., Peace Officer Standards and Training (POST)), or equivalent). This attribute is necessary to access services restricted to sworn law enforcement officers.

The eICAM function enables users to login once and access all participating systems for which they are authorized (with rules-based authentication) through single sign-on technology. Identity Access Management provides centralized administration of user identities, while allowing individual system owners to determine which users are authorized to access their system. The eICAM segment of LEEP supports secure information sharing between IdPs and SPs.

Security Identity Manager is an enterprise tool that provides effective identity management across the enterprise by improving compliance and security by being centrally located and provisioning to disparate directory stores. This software provides automatic identity creation, modification, recertification, and termination through user lifecycles, identity and password policies, customized schemas, modified views and customized workflows.

Security Verify Access (formerly Security Access Manager) provides user-friendly login and multifactor authentication to the www.cjis.gov login page. The upgraded software allows the FBI to adopt new security technologies to include two factor authentication and personal identity verification.

Federated Identity Manager provides a mechanism to pass secure identity information between federation entities. Federated Identity Manager enables users from a participating IdP to access services at a participating SP without a specific login at the SP, although the SP may request that the IdP re-authenticate the user. All IdPs must acknowledge that they are following the *CJIS Security Policy* before they are connected to LEEP and understand they are subject to audit by the CJIS Audit Unit.

The Security Verify Governance segment of LEEP manages the user account from request through vetting, creation, revetting, use or misuse, and finally deletion. It allows authorized personnel access to the user database without providing access to review and control user roles. Security Verify Governance allows the FBI to make appropriate access decisions and enable risk and compliance managers to quickly identify violations, identify analytics through visual insights into risky users, and identify insider anomalies and suspend accounts.

The Portal Services segment of LEEP provides a single point of entry for internal and external users to access SPs, which include both CJIS services and non-CJIS services. As the user interface, LEEP's Portal Service provides the gateway for IdP users to access resources hosted on LEEP. The Portal Service segment of the LEEP system does not have information that is retrievable by an individual user. Once LEEP validates a user's identity, the user is passed to the SP. The SP is then responsible for providing access management for the users it authorizes. The SP logs the users' activities within its service.

Leap Forms enables users to create web form applications for stand-alone use or for other end users. Non-technical users can create sophisticated web applications complete with forms, reports, and more. This service allows users to create web forms and to store the templates on LEEP for continued access. These forms could be shared across organizational and agency boundaries for daily use with operations and investigations. For example, users could use Leap Forms to develop an online application form to request access to a specific service or to create a registration form for a training event. The data collected on a created form will not be stored on LEEP at any time. To use a created form, the user launches a form, completes the form, and then receives the option to save the form to a local device (desktop or tablet) or to email the form to the user via their official email as designated in the LEEP user profile.

The primary purpose of collecting and sharing user information is to facilitate information sharing initiatives by connecting authorized LEEP users with systems and services maintained by the law enforcement, criminal justice, national security, and public safety communities to further their official missions. User information will not directly be used by LEEP to accomplish law enforcement or intelligence activities. Rather, LEEP authenticates the users' identity and credentials before passing user attributes to multiple agencies' information services where the information sharing takes place. The FBI will use the information shared through its own services on LEEP for further informing its criminal justice and national security efforts.

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. Chapter 33; 34 U.S.C. 10211; 44 U.S.C. 3101, 3301; 5 U.S.C. 301; Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. 3551 et seq.
Executive Order	Executive Order 13636
Federal regulation	28 CFR 0.85
Agreement, memorandum of understanding, or other documented arrangement	To become a federated IdP or a SP, non-FBI agencies are required to sign Memoranda of Understanding with the CJIS Division or have a signed CJIS User Agreement in place.
Other (summarize and provide copy of relevant portion)	Presidential Policy Directive 21, February 2013.

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.

LEEP maintains the PII of authorized users passed from the IdPs. Users who meet the criteria for LEEP membership include individuals affiliated with the criminal justice system, intelligence professionals, military personnel, and governmental agencies associated with infrastructure protection of the United States. On a case-by-case basis, other individuals offering direct support to the criminal justice system may be given access to LEEP. The criminal justice system includes, but is not limited to, law enforcement agencies (including campus police departments), correctional agencies, probation and parole entities, and prosecuting attorney's offices at the federal, state, local, tribal, or territorial levels. Intelligence professionals from federal, state, local, tribal, or territorial governmental agencies are also eligible for access to LEEP. On a case-by-case basis, intelligence analysts working as contractors for federal, state, local, tribal, or territorial law enforcement or government agencies may be given access to LEEP. Active duty and civilian military personnel are eligible for access to LEEP. Soldiers in a reserve or National Guard status may be granted access to LEEP on a case-by-case basis. Emergency management personnel, including public safety directors and commissioners, and employees of state and local emergency management and first responder offices are eligible for access to LEEP. Select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety missions may be granted access to LEEP on a case-by-case basis. Private sector user access to LEEP is limited to individuals with a demonstrated need for access. All private sector individuals must be sponsored by an authorized FBI LEEP user who certifies the private sector individual has a need to access LEEP. Foreign user access to LEEP is limited to non-U.S. citizens with a demonstrated need for access. Foreign users are limited to non-U.S. citizens vetted and employed by a U.S. criminal justice agency or approved U.S. agency IdP or sponsored foreign users with a LeepID account.[7]

The following user information may be collected and maintained by the system within the EIMS database:

- Full Name;
- Last four digits of the users' Social Security Number;
- Passport Number;
- Email 1 & 2 (business & personal);
- Date of Birth;
- Phone 1 & 2 (business & personal);
- Gender;
- Employer/Assignment Address;
- Employer/Assignment Phone;
- IdP;
- Federated IdP; and
- UID.

LEEP passes some user attributes, as part of a federated IdP SAML message, to SPs on behalf of the user. At a minimum the following attributes are exchanged: First name, Last Name, Employer, Email, Phone Number, and Local ID with IdP and federation ID being added by LEEP. Additional attributes may be included in the SAML message for authorization to an SP. For example, if an SP requires users to be sworn law enforcement officers, the SAML message must include an attribute indicating whether an individual is a sworn law enforcement officer. All information needed to access SPs must be included in the SAML message LEEP receives from the users' IdP. Only the information needed for security and auditing purposes is stored within the LEEP logs.

Users applying for a hosted CJIS IdP user account (e.g., LeepID accounts) complete an online application. The application collects the user's name, title, phone number(s), email address, citizenship, last four digits of social security number, date of birth, gender, passport number, whether

[7] Foreign user access to FBI information systems is addressed in FBI Policy 0607D, Section 8.3. In 2020, the FBI Chief Information Officer (CIO), the DOJ CIO, and the DOJ Department Security Officer granted LEEP an exemption to allow foreign user access. The FBI and DOJ review the exemption annually.

the applicant has specialized attributes (e.g., is a sworn law enforcement officer), and the user's employer and employer's contact information (e.g., name, phone number(s), address, and originating agency identifier (ORI)). Applicants not directly employed by a domestic criminal justice, public safety, or military agency must be sponsored by an authorized agency for LEEP access. If an applicant will be a sponsored user, the application also collects the sponsor's name and contact information. All foreign users requesting a LeepID account must be sponsored by an authorized FBI LEEP user who certifies that the foreign user has a need to access LEEP. Applications are stored within Appman.[8] Appman is used during the user vetting process. Once a user is vetted and granted a LeepID account, the user's information is removed from Appman and stored within the EIMS database.

Audit logs within LEEP contain a more common set of PII data used during day-to-day operations, typically encompassing the User ID and the IP address from which the user accesses LEEP. The audit logs track all user activity while on LEEP including login/logout times and SPs accessed. LEEP's audit logs do not track users' activity within a specific SP.

Although LEEP connects users with SPs, LEEP does not have access to any information shared within a specific SP. LEEP passes the user to the SP but once logged in to a specific SP, the SP is responsible for the users' actions and information sharing within its service. All SPs accessible via LEEP are responsible for completing required privacy documentation on their service, as necessary.

The chart below visibly depicts the types of information in LEEP.

(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, and D	
Date of birth or age	X	A, B, C, and D	
Place of birth	X	A, B, C, and D	
Gender	X	A, B, C, and D	
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	LEEP captures only the last 4 digits of users' social security numbers.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number	X	A, B, C, and D	

[8] Appman is a custom-built software interface tool which provides application management and support for initial and continued access requests to LEEP in support of the CJIS LeepID IdP. In the future, Appman will be replaced by Security Verify Governance.

(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

Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
E-mail address	X	A, B, C, and D	Users provide e-mail addresses; these can be personal or business.
Phone number	X	A, B, C, and D	Users provide their phone number; these can be personal or business. LEEP also collects the phone number for the users' agency.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B, C, and D	LEEP collects users' job titles, the name of the organization or agency that is the user's primary employer or the employer to which the user is currently assigned, and the ORI from the user's agency, if applicable.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			

(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

Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A, B, C, and D	
- **User passwords/codes**			
- **IP address**	X	A, B, C, and D	
- **Date/time of access**	X	A, B, C, and D	
- **Queries run**			
- **Contents of files**			
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		Hard copy: mail/fax		Online	X

Phone	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): As discussed, foreign users may provide their information for a LeepID account.					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify): As discussed above, select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety missions may be granted access to LEEP on a case by case basis.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	In addition to sharing user attributes with SPs, on a case-by-case basis, the FBI may share LEEP audit log data with federal, state, local, tribal, or territorial agencies for breach investigations or misuse investigations.
DOJ Components	X		X	
Federal entities	X		X	
State, local, tribal gov't entities	X		X	
Public				

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.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Use of LEEP information for litigation purposes is controlled by discovery processes, rules of evidence, and valid court orders.
Private sector			X	As discussed above, LEEP passes user attributes between approved IdPs and SPs. If a private sector service is approved to be a SP on LEEP, the private sector entity would receive user attributes for authentication purposes.
Foreign governments	X			
Foreign entities				
Other (specify):				

LEEP user attributes passed as SAML between IdPs and SPs are available to the FBI and all LEEP partner agencies. More detailed user information for hosted CJIS IdP accounts (e.g., Social Security Number, Passport number, and Date of Birth) is available only to FBI personnel involved in vetting hosted users and supporting LEEP operations. The LEEP Support Center provides 24/7 technical and program management support services for LEEP through a cooperative agreement with Louisiana State University. As an extension of the program management office, the LEEP Support Center provides operational support in a number of areas, such as website content management and development; technical support and troubleshooting; application management services; and field support. LEEP Support Center personnel have access to user data in the EIMS database, but most frequently access common data such as the user's full name, User ID, phone number, and email address. LEEP Support Center personnel retrieve user information by name or other personal identifier. Information in the EIMS database is only used to vet users, provide end user support, or in the event of a security incident. PAAM Services personnel have access to LEEP user applications in Appman. Users can view their own information through their LEEP profile on the LEEP homepage; however, LEEP does not provide general users access to any other users' information.

Audit logs are retained by enterprise logging authorities, specifically, Splunk Enterprise Logging.[9] Only LEEP system administrators have direct access to the audit logs. On a case-by-case basis, audit log information may be shared with other agencies and entities for misuse or breach investigations. LEEP System and Security Administrators can access audit logs by username or other

[9] The Department's Splunk Instance captures, indexes, and correlates "real-time" event data in a searchable repository from which IT and information security staff can generate graphs, reports, alerts, dashboards, and visualizations of various events. The Splunk solution provides insight into operational, security, and functional aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.

user attributes passed via SAML assertions.

The LEEP system has connections to the Internet and Intranet for access to services. All transmissions to and from the system are encrypted on LEEP assets and via the CJIS Division Shared Enterprise Network. Hosted CJIS IdP account applicants receive and submit their information through the LEEP user interface, www.cjis.gov. Notifications to users about the status of their accounts are sent via email from LEEP.

Users access LEEP from an internet capable device. Access to LEEP from external systems is accomplished through a secure authentication interface. LEEP provides secure access to numerous SPs for authorized LEEP users. LEEP streamlines access to the services housed within the CJIS Division and other SPs which support the criminal justice, national security, and public safety communities. The connections are made via eICAM allowing system to system connectivity. This connectivity permits the passing of identity information through a SAML message. Non-CJIS Division services are connected to LEEP via junctions which allow the secure passing of a SAML message.

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 FBI does not release information from LEEP for open data purposes or for research or statistical analysis purposes. Only authorized users, IdPs, and SPs, as discussed above, have access to LEEP information.

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.

LEEP passes user attributes between IdPs and SPs to authenticate a user's access to LEEP and SPs. Individual user information is required to authenticate the user for access. Individuals applying for a hosted CJIS IdP account receive a Privacy Act Statement on their application informing them why their information is requested and how it will be used. Federated user information is provided by the users' IdP. Notice may be provided to the federated IdP users via their agency's interfacing system when they provide their information as part of the application process. In addition, a privacy statement is linked at the bottom of the LEEP homepage informing LEEP users how LEEP uses their information. This Privacy Impact Assessment and the applicable System of Records Notices further inform users about how their information may be used or disclosed.

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.

Individuals applying for a hosted CJIS IdP account are advised that they do not have to provide the required information but failing to do so may result in the rejection of their application. IdPs automatically pass user attributes to LEEP upon users' login to the system. Users cannot decline to provide their attributes if they want to access LEEP. Individuals do not have the opportunity to consent to particular uses of the information. Individuals implicitly provide consent by voluntarily logging in to LEEP. LEEP's login page includes a warning banner informing users that they have no reasonable expectation to privacy regarding their actions on LEEP and that all activity is subject to monitoring and recording. Once logged in to LEEP, user attributes are automatically passed to any SP the user attempts to access. Users implicitly consent to the passing of their attributes by choosing the services to access. User attributes must be provided to each SP in order to authenticate the user's permission to access the service. Consequently, a user cannot decline to provide information to a service they attempt to access.

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.

LEEP users can view and update their information through their LEEP profile or by contacting the LEEP Support Center. Individuals may also request access to their records by following the guidance provided on the FBI's website at https://www.fbi.gov/services/records-management/foipa. A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR part 16. Individuals may mail, fax, or electronically submit a request, clearly marked "Privacy Act Access Request," to the FBI, ATTN: FOI/PA Request, Record/Information Dissemination Section, 200 Constitution Drive, Winchester, VA 22602-4693; facsimile: 540-868-4995/6/7; electronically: https://www.fbi.gov/services/records-management/foipa/requesting-fbi-records. A determination of whether a record may be accessed will be made after a request is received.

<u>Section 6</u>: 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):** LEEP is protected by "Defense in Depth"[10] strategies and continually monitored as a result of CJIS processes. LEEP's current Authority to Operate expires on 10/14/2022. LEEP is currently entering the iATO cycle. This is a new

[10] "Defense in Depth" is "an information security strategy that integrates people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization." NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, Appendix A (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

	process that will work through 4 phases (each 60 days in length) developed by OCIO. At the end of the cycle, a 3 year ATO is expected. Each cycle is an ATO extension as the program works through the requirements for each cycle. **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:** The LEEP Security Requirements Traceability Matrix is used to track security controls and any mitigations necessary to protect against identified risks.
	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:** Confidentiality - High, Integrity - High, Availability - High Justification: LEEP serves as the front door to a number of law enforcement information systems. It also serves as a point of authentication and authorization for a number of information systems, including web interfaces and server access for system administrators.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** LEEP is protected by "Defense In Depth" strategies and continually monitored as a result of CJIS processes.
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:** LEEP audit logs capture access to the system and the exchange of SAML messages between IdPs and SPs. Security personnel review audit logs using automated log aggregation toolsets. The Information System Security Officer (ISSO) reviews audit logs every 7 days, and the System Security Administrator (SSA) reviews audit logs daily.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All users are required to complete annual Information Security training and to agree to the LEEP Rules of Behavior which outline appropriate uses of the system.

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?

LEEP, as a FISMA reportable Information System with a Federal Information Processing Standards (FIPS) 199 data categorization rated overall HIGH (high for confidentiality, integrity, and availability), implements all required security controls in accordance with FBI Security Controls derived from NIST Special Publication 800-53. As an enterprise identity and access management solution, LEEP provides for strict adherence to technical, operational, and management security and privacy controls. LEEP uses access control lists to establish user roles. The user roles are then assigned to specific users to manage access to PII. The file systems and applications use the roles to limit access to PII to authorized users who have the appropriate role. Specifically, only authorized LEEP personnel and IT personnel who support LEEP have access to PII. LEEP restricts direct access to its audit logs to system administrators and system security administrators.

In order to mitigate threats to privacy in connection with the disclosure of information, CJIS has put in place a number of access controls within LEEP. LEEP collects and passes only minimum user attributes between IdPs and SPs to facilitate authentication of user access. LEEP uses multifactor authentication for all access to services via www.cjis.gov. For users accessing LEEP via federated IdPs, LEEP maintains only the user attributes passed from the federated IdPs. Once authentication to SPs is complete, federated user attributes are only maintained in restricted LEEP audit logs. Applicant information for hosted CJIS IdP user accounts is not disseminated outside of the FBI.

Additionally, the following controls have been put into place to prevent or mitigate threats to privacy:

- The CJIS Security Assessment team monitors system access to help mitigate the risk of inappropriate access to or use of the system.
- Users' PII is encrypted while transferred from system to system over networks.
- User information passed from IdPs to SPs only remains externally accessible while the user is being authenticated into a SP. Once the SP authenticates the user, information on that user is stored in restricted LEEP audit logs that are only directly available to limited FBI personnel. Once stored in audit logs, the data is only seen if there is a need to research an event for support or to investigate a potential security event. The Operating Systems, file systems, database management systems, and applications are all configured for role-based access that limits access to PII to only authorized users.
- Network and security device rules enforce access controls on all users.
- Security audit logs are implemented and monitored for unauthorized access. All audit logs are routinely reviewed for unauthorized access and anomalies.
- Users are provided with Rules of Behavior before access is granted to LEEP. Before being granted access to LEEP, users must agree to the Rules of Behavior and re-acknowledge them annually.
- Pursuant to the Rules of Behavior, users will immediately report known or suspected security incidents or improper use of LEEP to the LEEP Support Center, regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information.

- Non-FBI agencies are required to sign an MOU with the CJIS Division or have a signed CJIS User Agreement in place, both of which provide for termination of access to LEEP if there is a breach of their provisions.

The CJIS Audit Unit conducts triennial IT security audits of LEEP IdPs. All audits are conducted in terms of compliance under the requirements of the *CJIS Security Policy*. Privacy risks are further mitigated through required information security training for all users and by periodic security audits conducted by the CJIS Security Assessment team. Any allegations of misuse of CJIS systems are referred to the appropriate agency and CJIS Systems Agency[11] within the jurisdiction where the misuse occurred, and the FBI responds to all such allegations.

LEEP currently resides on the CJIS Division Common Compute Platform at the CJIS Division. Data is stored and backed up securely on the CJIS Division Enterprise Storage Services (ESS). The data is unencrypted at rest; however, the system is located in a secure access facility. ESS connects to other systems/services through the CJIS Shared Enterprise Network. A combination of Splunk and Nagios is used to ensure system availability through a series of monitoring capabilities and reports provided in real-time. All system security logs are forwarded to the CJIS Division and FBI Security Operations Centers for continued cyber security monitoring.

LEEP is in the process of transitioning to a cloud environment. When fully transitioned, LEEP will use Amazon Web Services' (AWS) government cloud (GovCloud) environment as infrastructure-as-a-service. AWS owns the AWS GovCloud environment. Access to FBI information in the cloud infrastructure is limited to FBI personnel. Access by FBI personnel to specific FBI applications and datasets is determined at the application and dataset level. Audit logs and user login identifiers are collected and maintained by both the FBI and AWS; however, AWS personnel do not have the capability to access FBI applications or datasets, or to audit user activity therein. Data in transit is encrypted using Transport Layer Security FIPS 140-2 encryption, and all interconnections between the AWS GovCloud and the FBI utilize firewalls and security filtering. LEEP will also use FIPS 140-2 compliant encryption at rest for all data in the cloud.

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.)

User information passed from IdPs to SPs only remains externally accessible while the user is being authenticated into an SP. Once the SP authenticates the user, information on that user is stored in restricted LEEP audit logs that are only directly available to limited FBI personnel. LEEP audit logs are retained for 25 years. Hosted CJIS IdP approved applications and account data is deleted six years after a user account is terminated or when no longer needed for investigative or security purposes, whichever is later. Rejected applications for hosted CJIS IdP accounts are deleted after two years or when no longer needed for investigative or security purposes, whichever is later. See NARA Job

[11] CJIS Systems Agencies are the local, state, tribal, territorial or federal agencies which enter into CJIS User Agreements with FBI CJIS and take responsibility for their agency users' access and use of CJIS systems. They also actively participate in the FBI CJIS Advisory Policy Board, helping FBI CJIS develop the CJIS Security Policy and CJIS System program policies. *See* www.fbi.gov for details.

Number N1-065-06-001, available at: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-06-001_sf115.pdf.

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:

JUSTICE/FBI-004, *FBI Online Collaboration Systems*, 82 Fed. Reg. 57291 (Dec. 4, 2017);

JUSTICE/DOJ-002, *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, 86 Fed. Reg. 132 (Jul. 14, 2021).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

LEEP collects information directly from individuals applying for hosted CJIS IdP accounts. Collecting information directly from the applicants mitigates the risk that information may be inaccurate. However, because LEEP allows individuals to directly apply for hosted CJIS IdP accounts, there is a risk that individuals unauthorized to access LEEP may apply for an account. Through its vetting procedures, LEEP conforms to the NIST 800-63 Identity Assurance Level 2 standard that involves:

1. Resolution - capturing identity information to uniquely distinguish the individual among a given population;
2. Validation - determining the authenticity, validity, and accuracy of the identity information and relating it to a real-life subject; and

3. Verification - forming a linkage between the claimed identity and real-life existence of the subject presenting the evidence.

These steps work to ensure only authorized individuals receive an account. Vetting procedures include requiring confirmation of an applicant's employment and need to access LEEP, as established by a pre-approved LEEP contact within an authorized agency. In addition, LEEP annually conducts its vetting procedures on all hosted CJIS IdP users to ensure the individuals are still employed at authorized agencies and that users still have a need to access LEEP. Similarly, federated IdPs must comply with LEEP's vetting requirements and re-vet their users on an annual basis. In addition, FBI also works with IdPs on a continual basis, and can disable accounts in response to unauthorized use, access, etc. This ensures LEEP user attributes are kept accurate and up-to-date and that only authorized individuals with a need to access LEEP have the ability to do so.

To protect applicants' privacy, LEEP requests only the minimal amount of PII necessary to appropriately vet an applicant. Once granted a hosted CJIS IdP account, LEEP passes only the minimum user attributes required to SPs to allow user access. More detailed user information for hosted CJIS IdP accounts (e.g., last four Social Security Number, Passport number, and Date of Birth) remains available only to FBI personnel involved in vetting hosted CJIS IdP users and supporting LEEP operations.

LEEP's primary purpose is to enable information sharing by securely enabling, protecting, and managing access to systems by federal, state, local, tribal, and territorial criminal justice, national security, and public safety communities nationwide. Consequently, there is a risk that unauthorized individuals will attempt to gain access to LEEP through social engineering[12] individuals eligible for LEEP access. To mitigate the risk of social engineering, LEEP mandates that the components of identity assurance follow the National Institute of Standards and Technology (NIST) guidelines for all access to portal services.[13] This is accomplished through multifactor authentication including the issuance of a one-time password for users that access LEEP. In addition, the FBI CJIS Division chose the portal federation model to mitigate threats to privacy. By using LEEP as a gateway to the other information sharing systems, the FBI helps further mitigate potential threats to privacy by reducing the need for agencies' users to maintain multiple accounts and passwords. The user is connected and logged in through their agency's network, with their agency's credentials, through the trusted interface. Only the minimum information necessary (e.g., name, email address, telephone number, name of the user's employer, system audit data) is required from the partnered information sharing systems. User information passed from IdPs to SPs only remains externally accessible while the user is being authenticated into an SP. Once the SP authenticates the user, information on that user is stored in restricted LEEP audit logs that are only available to limited FBI personnel. Regardless of these mitigation efforts certain risks for social engineering, malware, and hacking are inherent to any web-facing portal.

Potential threats to privacy may result from improper access to the data or misuse of information in the LEEP system or any connected information sharing systems accessible through

[12] NIST defines social engineering as "an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks." NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide (Aug. 2012), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
[13] *See* NIST SP 800-63C-3, Digital Identity Guidelines (March 2020).

LEEP. These threats could compromise the security of LEEP users' PII. To protect user information and the LEEP system, the FBI has implemented security features required for system certification and accreditation. Both IdPs and SPs interfacing their IT systems with LEEP are subject to all applicable privacy and security requirements, which include encryption of users' PII during transfer from system-to-system; periodic security audits conducted by the CJIS Security Assessment team; annual information security training for all users; network and security device rules that enforce role-based access controls on all users; and adherence to the LEEP Procedure and Operations Manual, the CJIS Security Policy, and/or the NIST Special Publication 800-63.2 Electronic Authentication Guideline, as well as FBI Policy for FBI IdPs. IdPs and SPs must also have advanced authentication in place for their connection. FBI systems connected to LEEP are documented via an Electronic Communication and DOJ systems are documented with a letter or an MOU. Non-FBI agencies are required to sign an MOU with the CJIS Division or have a CJIS User Agreement in place, both of which provide for termination of access to LEEP if there is a breach of their provisions.