Federal Bureau of Investigation

Privacy Impact Assessment
for the
Law Enforcement Enterprise Portal

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: [July 3, 2019]

EXECUTIVE SUMMARY

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 local, state, tribal, territorial, and federal agencies. Select international entities and private sector individuals also access LEEP to share information with local, state, tribal, territorial, and federal 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 1: Description of the Information System

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

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 local, state, tribal, territorial, and federal criminal justice, national security, and public safety communities nationwide. Select international entities and private sector individuals also access LEEP to share information with local, state, tribal, territorial, and federal agencies. LEEP is a technical architecture-aligned solution that provides the FBI and other local, state, tribal, territorial, and federal agencies with the able to identify, monitor, and manage subjects that access FBI resources. This set of Enterprise Identity Management Services (EIMS) include Identity Access Management, Security Identity Management, Portal Services, Federated Identity Management Services, and the Forms Experience Builder, detailed below, are 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

[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.

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

Service Providers (SPs).[4] **Hosted IdPs** (e.g. LeepID IdP, National Instant Criminal Background Check (NICS) ECheck, Cyberhood Watch) 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] 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.

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

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 Governance and Policy Guidance documents, 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.

Industry LEEP (iLEEP), a specialized version of LEEP, enables private and critical infrastructure industry partners to access select LEEP SPs. It is supported by the same technical software and hardware which makes up LEEP. iLEEP facilitates secure and trusted electronic information sharing between the owners, operators, and chief security officers of national key asset and critical infrastructure sectors (e.g. chemical, communications, nuclear, defense, and energy facilities) and criminal justice and national security agencies. iLEEP can be accessed by criminal justice, national security, first responder, and private industry users alike through the FBI Office of Private Sector National Strategic Partnership Unit's InfraGard[6] network,

[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 standardize 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] InfraGard is an information sharing and analysis network servicing the interests and combining the knowledge base of a wide range of members. InfraGard is a partnership between FBI and the private sector. InfraGard is an association of business, academic institutions, local and state law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the Unites States. InfraGard

Cyberhood Watch,[7] or other authorized IdPs. Private industry users accessing SPs via iLEEP see only those SPs relevant to the users' areas of responsibility. iLEEP directs certain private sector partners to select SPs. iLEEP user information is stored within LEEP. The privacy implications and mitigations discussed in this PIA apply equally to LEEP users and iLEEP users, unless otherwise stated.

The Identity Access Management function enables users to login once to the portal 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 Federated Identity Management Service segment of LEEP supports secure information sharing between IdPs and SPs. Federated Identity Management Service provides a mechanism to pass secure identity information between federation entities. Federated Identity Management Service 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 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.

The Forms Experience Builder enables users to create web form applications for stand-alone use or for other end users. Non-technical users are able to create sophisticated web applications complete with forms, reports, and more. This service will allow 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. The data collected on a created form will not be stored on LEEP at any time. To use a created form, the user will launch a form, complete the form, and then be given the option to save the form to a local device (desktop or tablet) or to email the form to the user via his/her official email as designated in the LEEP user profile.

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

LEEP maintains the PII of authorized users passed from the IdPs. Users who meet the criteria for a LeepID account 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

Chapters are geographically linked with FBI Field Office territories. InfraGard has separate privacy documentation.

[7] Cyberhood Watch provides a secure forum where trusted private industry participants can share cyber security best practices, threat intelligence information, report suspicious network activity, and interact with FBI special agents and cyber intelligence analysts. Cyberhood Watch has separate privacy documentation.

departments, correctional agencies, probation and parole entities, and prosecuting attorney's offices on the federal, state, or local levels. Intelligence professionals from local, state, tribal, territorial, or federal governmental agencies are also eligible for access to LEEP. On a case by case basis, intelligence analysts working as contractors for local, state, tribal, territorial, or federal 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. 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. Private sector access to iLEEP is controlled by specific IdPs (e.g. InfraGard) which vet users' need to access the select services available on iLEEP.

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

- Full Name;
- 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 a 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 users IdP. Only the information needed for security and auditing purposes is stored within the LEEP logs.

Users applying for a hosted IdP user account (e.g. a LeepID account) complete an online application. The application collects the user's name, title, phone number(s), email address, citizenship, social security number, date of birth, gender, passport number, whether 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 for LEEP access. If an applicant will be a sponsored user, the application also collects the sponsor's name and contact information. 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 also 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 into 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.

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

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 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. 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. Information in the EIMS database is only used to vet users, provide end user support, or in the event of a security incident. Membership 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 access to the audit logs.

[8] Appman is a custom-built software interface tool which provides application management and support for initial and continued access requests to LEEP.

[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

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

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 service. The service is then responsible for providing access management for the users it authorizes. The SP then logs the users' activities within its service.

LEEP Support Center personnel retrieve user information by name or other personal identifier. Audit logs can be retrieved by username or other user attributes passed via SAML assertions.

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

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 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.

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

LEEP 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 (SOC) for continued cyber security monitoring.

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 Federated Identity Management Services 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.

Section 2: Information in the System

aspects of the environment. More information on Splunk can be found at https://www.splunk.com/.

2.1 Indicate below what information is collected, maintained, or disseminated.

(Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license		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		Place of birth	X	Financial info	
Alias		Home address		Medical information	
Gender	X	Telephone number	X	Military service	
Age		Email address	X	Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation		Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates			
Other work-related data (specify): The name of the organization or agency that is the user's primary employer or the employer to which the user is currently assigned. LEEP will also collect the Originating Agency Identifier from the user's agency, if applicable.					

Distinguishing features/Biometrics					
Fingerprints		Photos		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	X	Queries run		Contents of files	
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		Online	X
Telephone	X	Email	X		
Other (specify):					

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	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.					

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.)

LEEP collects information directly from individuals applying for hosted IdP LEEP 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 IdP accounts, there is a risk that individuals unauthorized to access LEEP may apply for an account. Through its vetting procedures, LEEP ensures that only authorized individuals receive a LEEP account. Vetting procedures include requiring confirmation of an applicant’s employment by a pre-approved LEEP contact within an authorized agency. In addition, LEEP annually conducts its vetting procedures on all hosted 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 revet their users on an annual basis. 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 an account, LEEP passes only the minimum user attributes required to SPs to allow user access. More detailed user information for hosted IdP accounts (e.g. Social Security Number, Passport number, and Date of Birth) remains available only to FBI personnel involved in vetting hosted IdP users and supporting LEEP operations.

The primary purpose of LEEP is to protect and manage access to systems by local, state, tribal, territorial, and federal 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[10] 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.[11] This is accomplished through multifactor authentication including the issuance of a one-time password for users that access LEEP. Additionally, 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 a 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.

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			
X	For criminal law enforcement activities	□	For civil enforcement activities
X	For intelligence activities	□	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest	X	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): To reduce the need for agencies' users to maintain multiple accounts and passwords.		

[10] 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.
[11] *See* NIST SP 800-63-3, Digital Identity Guidelines (June 2017).

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

The 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 passes 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.

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

Authority		Citation/Reference
X	Statute	28 U.S.C. 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.*
X	Executive Order	Executive Order 13636
X	Federal Regulation	28 CFR 0.85
X	Memorandum of Understanding/agreement	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.
X	Other (summarize and provide copy of relevant portion)	Presidential Policy Directive 21, February 2013.

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.)

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 available to limited FBI personnel.

LEEP audit logs are retained for 25 years. Hosted IdP approved applications and account data is deleted 6 years after a user account is terminated or when no longer needed for investigative or security purposes, whichever is later. Rejected applications for hosted IdP accounts are deleted after 2 years or when no longer needed for investigative or security purposes, whichever is later.

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.]

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 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. The LEEP program office, the Online Services and Operations Unit, resides at CJIS to coordinate FBI's technical, policy, and security compliance.

In addition, all LEEP users annually acknowledge the LEEP Rules of Behavior. The Rules of Behavior require all users to 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.

To further minimize unauthorized access and use of user PII and LEEP, 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 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. LEEP Operating Systems, file systems, database management systems, and applications are all configured for role-based access which limits access to PII for only those authorized users. Network and security device rules enforce access controls on all users. Security audit logs are implemented and monitored for unauthorized access.

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.

<u>Access controls</u>

X	Access Enforcement: the system employs role-based access controls and enforcement mechanisms for PII.
X	Separation of Duties: users of de-identified PII data are not also in roles that permit them to access the information needed to re-identify the records.
X	Least Privilege: user roles enforce the most restrictive set of rights/roles for each user group.
X	Remote Access: remote access is prohibited or limited to encrypted communication channels.
X	User-Based Collaboration and Information Sharing: automated mechanisms are in place for matching PII access authorizations to access restrictions, such as contractual/MOU/MOA requirements.
	Access Control for Mobile Devices: Federated IdPs permit access to authorized users through mobile devices. LEEP does not ensure the security of the user device. If a user accesses LEEP via agency owned mobile assets/devices, the device is controlled at the agency level. LEEP allows users to access the system from any public internet service provider on any internet capable device.

<u>Audit controls</u>

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

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified and authenticated before accessing PII; remote access requires 2-factor authentication and 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.
Media controls are inherited from ESS/Enterprise Storage Area Network.	

Data Confidentiality controls

	Transmission Confidentiality: Traffic to and from LEEP is negotiated at the highest level of encryption when possible.
X	Protection of Information at Rest: Information is not encrypted at rest. LEEP servers reside in a physically restricted facility.

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			X	
Federal entities			X	
State, local, tribal gov't entities			X	
Public				
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):				

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.]

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 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 IdP user accounts is not disseminated outside of the FBI.

All users are provided with Rules of Behavior the first time they access the system and annually thereafter. The Rules of Behavior require users to 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. All audit logs are routinely reviewed for unauthorized access and anomalies. The CJIS Audit Unit audits CJIS Systems for which they have been assigned responsibility for auditing. The CJIS Audit Unit audits two CJIS Systems which are LEEP SPs as part of their triennial audits, NICS and N-DEx. The CJIS Audit Unit conducts 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[12] within the jurisdiction where the misuse occurred, and the FBI responds to all such allegations. Additional security controls in place to mitigate threats to privacy are discussed in more detail in Sections 2 and 3, above, and Section 6 below.

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: Individuals applying for a hosted IdP account receive a notice on the application informing them why their information is requested and how it will be used. Individual user information is required to authenticate the user for access. Federated user information is provided by the users' network. Notice may be provided to the federated IdP users via their agency's interfacing system when they provide the 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.
	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, in part, individuals have the opportunity to decline to provide information.	Specify how: Individuals applying for a hosted 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.
X	No, in part, individuals do not have the	Specify why not: IdPs automatically pass

[12] 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.

	opportunity to decline to provide information.	user attributes to LEEP upon users' login to the system. Users cannot decline to provide their attributes if they want to access LEEP.

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

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Individuals do not have the opportunity to consent to particular uses of the information. Individuals implicitly provide consent by voluntarily logging into 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.

5.3 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.

As discussed above, 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 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 or Records Notice further inform users about how their information may be used or disclosed.

Individuals provide consent for LEEP's use of their information by voluntarily logging into

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 into 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 he attempts to access.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted.	
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: The LEEP Security Requirements Traceability Matrix is used to track security controls and any mitigations necessary to protect against identified risks.	
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	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: LEEP is protected by "Defense In Depth" strategies and continually monitored as a result of CJIS processes. LEEP's current Authority to Operate expires 05/17/2019.	
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: LEEP audits are retained for a minimum of one year and security personnel review audit logs using automated log aggregation toolsets.	
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.
	X	Other (specify): 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 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.]

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, Revision 4. 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 access to its audit logs to system administrators and system security administrators. 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 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.
- 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.

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 Online Collaboration Systems*, **JUSTICE/FBI-004**, 82 Fed. Reg. 57291 (Dec. 4, 2017) *Department of Justice Computer Systems Activity and Access Records*, **JUSTICE/DOJ-002,** 64 Fed. Reg. 73,585 (Dec. 30, 1999), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001) and 72 Fed. Reg. 3410 (Jan. 25, 2007)
□	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.

As discussed above, LEEP Support Center personnel retrieve user information from EIMS and associated user interfaces by name or other personal identifier. Audit logs can be retrieved by username or other user attributes passed via SAML assertions.