Federal Bureau of Investigation

Privacy Impact Assessment
for the
[Law Enforcement Online (LEO)]

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 19, 2022]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Law Enforcement Online (LEO)[1] is a controlled access network that provides an Internet-accessible focal point twenty-four hours a day, seven days a week, for Controlled Unclassified Information (CUI) communication and information sharing among law enforcement and national security agencies. These include federal, state, tribal, foreign, local, and international criminal justice agencies, intelligence agencies, as well as military, other government personnel, and sponsored entities involved in criminal justice and national security matters. LEO provides a secure communications network for online information sharing supporting antiterrorism, intelligence, law enforcement, criminal justice, and public safety communities on a national and international level.

This Privacy Impact Assessment (PIA) addresses the types of personally identifiable information (PII) shared on LEO and the controls in place to protect it. The PII in LEO includes criminal justice and national security information, as well as sensitive personal information such as names, social security numbers, biometrics, financial account information, and medical information.

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 Criminal Justice Information Services (CJIS) Division, Data Sharing and Services Unit (DSSU) manages LEO. The FBI CJIS Division Information Technology Management Section Law Enforcement Technical Services Unit provides development, operation, maintenance, and enhancement for the system.

As noted above, LEO is a twenty-four hours a day, seven days a week, online (near real-time), controlled access network providing an Internet-accessible focal point for electronic CUI communication and information sharing for federal, state, tribal, foreign, local, and international criminal justice agencies, intelligence agencies, as well as military, other government personnel, and sponsored entities (including private sector individuals) involved in criminal justice and national security matters. LEO supports antiterrorism, intelligence, law enforcement, criminal justice, and public safety communities on the national and international level by providing and maintaining a secure communications network.

LEO contains three separate services which promote collaboration and information sharing among its users: Special Interest Groups (SIGs), Virtual Command Centers (VCCs), and @leo.gov email. Users access the LEO services via the FBI's Law Enforcement Enterprise Portal (LEEP),[2] which is a web-based gateway for authorized LEEP federation users to access multiple systems and services by using single sign-on technology.[3] Vetted and authorized users access LEO via industry-

[1] LEO used to be called LEO Services as reflected in the PIA dated July 16, 2019.
[2] LEEP has separate privacy documentation.
[3] "Single sign-on technology" is a standard industry term used to describe a technology that "employs a central

standard personal computers, laptops, tablets and smart phones through the LEEP federation Identity Providers (IdPs).[4] Web-based information is transmitted through a standard web browser interface which requires a Transport Layer Security (TLS) version 1.2 connection to the LEEP portal.

Special Interest Groups (SIGs)

A SIG is a web-based, controlled-access, information-sharing platform designed to allow federal, state, local, tribal, and international partners to share and store information to facilitate and enhance strategic collaboration among the criminal justice, national security, and public safety communities. LEO hosts three types of SIGs: unrestricted SIGs that are open to all LEEP federation members; restricted SIGs which allow any user to request access to the private area of the SIG; and private SIGs which are only accessible or viewed by its members. Private SIGs are hidden and cannot be seen by all LEEP federation users. Only users invited to join the private SIG can access the private SIG.

All SIGs contain at least one moderator (owner). The moderator manages the SIG within LEO and chooses whether and/or how to share certain information with SIG members. If a moderator does not want information shared within their SIG, the moderator will not post the information. Moderators determine the type of information contained within a SIG based on the purpose of their SIG. The type of information shared within SIGs includes, but is not limited to, schedules, maps, contact lists, pictures of all types (locations, suspects, witnesses, security personnel, hospitals, and evacuation routes), unclassified intelligence articles and reports, arrest reports, information on open criminal investigations, and case reports. Within the SIGs, users can search for information using keyword searches.

Only the SIG moderator can upload information or request information be added to the SIG. The SIG moderator can directly upload content to the SIG they moderate. The file selected to be uploaded is passed through the system's classification filters prior to completing the upload to the operational environment. If the file contains classification markings, the file is quarantined and security is notified. The SIG moderator can also provide information for the SIG to the FBI Content Team, which passes the information through classification filters. Once the information passes through the classification filters, the content is uploaded and posted within the moderated SIG. The FBI Content Team does not alter the content of the information provided for posting. The SIG moderator is responsible for the contents of the shared information.

SIGs also provide their users with LEO Listservs functionality. A listserv is a mailing list that allows members to easily reach everyone subscribed to the listserv. Listservs are created with each SIG and can also be requested outside of SIGs. Listserv messages are delivered by moderators or with a moderator's approval.

---

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, Special Publication 800-36, Guide to Selecting Information Technology Security Products (Oct. 2003), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-36.pdf.

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

Virtual Command Center (VCC)

LEO also hosts the VCC application. The VCC application is a tactical, real-time collaboration tool that facilitates shared situational awareness and incident management, including threat monitoring and live updates. The VCC constitutes a secure common operating platform providing seamless, real-time, situational awareness, and critical incident management and fosters multi-agency collaboration allowing federal, state, local, and tribal users to seamlessly share data. The VCC provides a secure platform for immediate and effective dissemination of information and unclassified intelligence. All VCCs are either restricted or private; individuals must apply for access to a specific VCC and only authorized LEEP users with a need to access a specific VCC will have access. The VCC owner controls who may access their VCC.

The VCC contains readily available reference materials which are appropriate to particular events, venues, or interagency information sharing. The VCC stores information entered by users, which may include PII, such as identification of suspects or missing persons, and any case, incident, or operation relevant information. Certain information, such as incident status, free text narrative, and information concerning how the incident was received, is presented through an "Events Board" which is a virtual bulletin board within the VCC viewable by LEO users with access to the specific VCC. Other information elements, such as agency name, agency phone number, and a map of the surrounding event locations are accessible by navigating through the VCC and selecting appropriate tabs to display the information. The types of information shared within VCCs includes, but is not limited to, schedules, maps, contact lists, pictures of all types (locations, suspects, witnesses, security personnel, hospitals, and evacuation routes), unclassified intelligence articles and reports, arrest reports, information on open criminal investigations, and case reports. Within the VCC, users can search for information via keyword searches. Similar to SIGs, VCCs may also use LEO Listservs to disseminate information to their members.

There are three roles within a VCC: administrator, poster, and viewer. Once inside the VCC, administrators and posters can directly add content to the VCC. Once a VCC is no longer required for a specific event, the VCC administrator must close the VCC. The VCC administrator is responsible for downloading and saving any information from the VCC which may be needed for operational and record keeping purposes. VCC administrators may download information from the Events Board and static data posted to the VCC to Excel or save it as a .pdf document.

@leo.gov Email

With access to LEEP, users can qualify for and receive an @leo.gov email address. The @leo.gov email allows users to send and receive email with any other Internet accessible email address. The @leo.gov is an unclassified email system and, therefore, scans for classified markings in the body of the email and text-based attachments. @leo.gov email includes an address book which users can use to find contact information for other individuals with @leo.gov email addresses.

LEO members may use their LEO email accounts to send email to other LEO members or to share information externally with non-LEO email accounts. Shared information may include documents, articles, law enforcement forms, spreadsheets, presentations, images, and any other shared files made available to LEO users by other LEO users, for either online viewing or downloading.

Email is transmitted through email clients and servers over the Internet. If the recipient email domain supports TLS connections, LEO establishes a TLS connection with the recipient domain to ensure that the information (emails) is transmitted through an encrypted session. If, however, the recipient domain does not support TLS connections, the information (emails) is sent in clear text to the recipient domain. @leo.gov email also supports incoming TLS connections for those originating email services which support outgoing TLS connections.

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
x	Statute	28 USC Chapter 33; 44 USC 3101; 34 U.S.C. § 10211
	Executive Order	
x	Federal Regulation	28 CFR 0.85; 28 CFR Part 20
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

LEO is a collaboration tool for authorized LEEP federation users for criminal justice, national security, intelligence, public safety, and other official business purposes. By design, the range of authorized purposes for use of LEO is extremely broad and the information involved is likewise extremely broad. Each time a LEO user accesses any of LEO's information-sharing applications, LEO stores user-provided data. The content of the data shared via LEO's applications vary widely depending on the purposes for which it is shared. For example, a LEO user may post a question on a virtual bulletin board about whether any other user knows how to apply for a search warrant to access Internet open-source data. Another user may post PII in a VCC on a suspect for whom police are searching, including the suspect's name, physical description, and date of birth. LEO's content, which is accessible to users for viewing, printing, or downloading, includes documents, spreadsheets, presentations, images, and other files. Users may include all types of PII about themselves or third parties, including names, aliases, all types of personal identification numbers, financial information, gender, date and place of birth, age, country of origin, nationality, address, telephone numbers, email addresses, military history, medical information, occupation, place of employment, photos, all types of

physical characteristics, and activities.

The @leo.gov address book contains a user's PII only if the @leo.gov email account is active. The @leo.gov address book includes the following PII on individuals with an @leo.gov email address: name, title, email address (@leo.gov only), telephone numbers, postal address, and login ID. If the user has not accessed any of the LEO services within 180 days, their account becomes inactive, and the individual's information is no longer searchable in the address book.

In addition, LEO creates user access and activity records to ensure that LEO is being used appropriately and only by authorized users. Access to all LEO data is audited. An audit log of what information was accessed, what information was changed/added/deleted, and when these activities occurred is maintained in various audit logs depending on the application in use. The identity of the LEO user making these changes is recorded in the audit logs. LEO system administrators monitor the audit logs via direct access to the system through internal resources, such as workstation-related tools operated and maintained within the CJIS Division Unclassified Network enclave.

The chart below visually depicts the types of information that may be included in LEO.

(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	X	A, B, C and D	
Religion	X	A, B, C and D	
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	
Tax Identification Number (TIN)	X	A, B, C and D	
Driver's license	X	A, B, C and D	
Alien registration number	X	A, B, C and D	
Passport number	X	A, B, C and D	
Mother's maiden name	X	A, B, C and D	
Vehicle identifiers	X	A, B, C and D	
Personal mailing address	X	A, B, C and D	
Personal e-mail address	X	A, B, C and D	
Personal phone number	X	A, B, C and D	
Medical records number	X	A, B, C and D	
Medical notes or other medical or health information	X	A, B, C and D	
Financial account information	X	A, B, C and D	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Applicant information	X	A, B, C and D	
Education records	X	A, B, C and D	
Military status or other information	X	A, B, C and D	
Employment status, history, or similar information	X	A, B, C and D	
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	
Certificates	X	A, B, C and D	
Legal documents	X	A, B, C and D	
Device identifiers, e.g., mobile devices	X	A, B, C and D	
Web uniform resource locator(s)	X	A, B, C and D	
Foreign activities	X	A, B, C and D	
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	
Juvenile criminal records information	X	A, B, C and D	
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C and D	
Whistleblower, e.g., tip, complaint or referral	X	A, B, C and D	
Grand jury information	X	A, B, C and D	
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	
Procurement/contracting records	X	A, B, C and D	
Proprietary or business information	X	A, B, C and D	
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C and D	
Biometric data (while not all of the data below may be applicable, users are not limited or prohibited from entering the below):		A, B, C and D	
- **Photographs or photographic identifiers**	X	A, B, C and D	
- **Video containing biometric data**	X	A, B, C and D	
- **Fingerprints**	X	A, B, C and D	
- **Palm prints**	X	A, B, C and D	
- **Iris image**	X	A, B, C and D	
- **Dental profile**	X	A, B, C and D	
- **Voice recording/signatures**	X	A, B, C and D	
- **Scars, marks, tattoos**	X	A, B, C and D	
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C and D	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **DNA profiles**	X	A, B, C and D	
- **Other (specify)**	X	A, B, C and D	
System admin/audit data:		A, B, C and D	
- **User ID**	X	A, B, C and D	
- **User passwords/codes**	X	A, B, C and D	
- **IP address**	X	A, B, C and D	
- **Date/time of access**	X	A, B, C and D	
- **Queries run**	X	A, B, C and D	
- **Content of files accessed/reviewed**	X	A, B, C and D	
- **Contents of files**	X	A, B, C and D	
Other (please list the type of info and describe as completely as possible):			
Sworn Law Enforcement information; Intelligence Analyst information; ORI# (originating agency identifier)	X	A, B, C and D	
Federation ID, which is a unique alphanumeric identification assigned to users by the system. It is required for access.	X	A, B, C and D	

LEO only requires its users to provide their name, phone number, email address, and agency affiliation. All other information about users is voluntarily provided. The purpose of SIGs and VCCs is to provide collaboration among and between the FBI and its partners for official purposes. Therefore, it is possible the above types of information about non-LEO users may be shared within SIGs and VCCs to assist agencies in performing their official duties. However, LEO only supports text-based searches and retrieval of information. Information cannot be retrieved biometrically (e.g., by face recognition technology or the comparison of fingerprint images).

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		Email			
Other (specify):					

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

Government sources:					
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):					

Non-government sources:					
Members of the public	x	Public media, Internet	x	Private sector	x
Commercial data brokers	x				
Other (specify): These sources may provide information to authorized LEO users who may share the information within LEO. Limited private sector individuals may have sponsored access to LEO.					

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	
DOJ Components	X		X	
Federal entities	X		X	
State, local, tribal gov't entities	X		X	
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X		X	Prosecuting attorneys, Attorney Generals Offices, and courts are authorized criminal justice users of LEO. Use of LEO information for litigation purposes is controlled by discovery processes, rules of evidence, and valid court orders.

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.**
Private sector	X		X	LEO users include select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety missions. LEO users may share information from LEO with non-LEO users for criminal justice or other official business purposes.
Foreign governments	X		X	LEO users include foreign law enforcement officers and analysts sponsored by an authorized FBI LEEP user or foreign users who access LEEP through an authorized IdP and are vetted by that IdP.
Foreign entities	X			
Other (specify):	X			On a case-by-case basis, LEO users may share information from LEO with non-LEO users for criminal justice or other official business purposes.

LEO is a controlled access information sharing platform that employs role-based access controls to manage access to information. LEEP provides authentication control to LEO, as well as other FBI resources. All LEO users must have access to LEEP through their own agency's IdP or through a LEEP ID account. LEO user groups are categorized into two major groups: general and privileged. These user groups have differing roles, permissions, and user rules of behavior when accessing the system.

General users have access to common applications within the system. Roles and permissions allow general users to access additional areas within LEO such as SIGs and VCCs. General users are authorized LEEP federation users. Individuals are authorized to access LEEP if they are affiliated with the criminal justice system, intelligence communities, 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 and LEO. This includes approved foreign users. 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 offices at the federal, state, local, tribal and territorial

(FSLTT) levels. Intelligence personnel from FSLTT governmental agencies are also eligible for access to LEEP and LEO. On a case-by-case basis, intelligence analysts working as contractors for FSLTT government agencies may be given access to LEEP and LEO. Active duty and civilian military personnel are eligible for access to LEEP and LEO. Soldiers in a reserve or National Guard status may be granted access to LEEP and LEO 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 and LEO. 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 and LEO.

In order to properly limit LEO access to criminal justice, military, governmental personnel, and active LEEP account holders (critical infrastructure, private emergency medical service organizations, private sector, forensic dentists, coroners, etc.), individuals must request a LEEP account through either their agency IdP or by completing an individual LEEP ID Account application. LEEP accounts are only granted after the IdP or the DSSU membership team vets the individual to ensure he or she meets the LEEP membership criteria.

General users have access to all public SIGs. Restricted and private SIGs restrict access to LEEP federation users who have a vested interest in a particular special interest group and have access to the private and/or restricted SIG for which they have been approved. SIG moderators determine who can access their restricted or private SIGs based on the user's need to know the information shared within the SIG. Each SIG has at least one SIG moderator to manage the site by filtering and/or being responsible for information posted for the SIG, approving or denying users' requests for access, and enforcing proper use and conduct of the SIG. Similarly, VCC Administrators control access to their VCCs. VCC Administrators only provide VCC access to LEO members with a vested interest in the VCC, based on a need to know.

Privileged Users are system and database administrators who support LEO. Privileged users have access to member, content, and application controls, such as creating and disabling accounts, resetting user passwords, posting documentation and managing content on the system, and maintenance of applications on the system, such as SIGs and VCCs. Privileged users have heightened access to all SIGs based on their need to manage the entire system. Such users include: The LEEP Help Desk; DSSU personnel; and LEO system administrators. LEEP Help Desk staff are contract personnel responsible for answering help desk calls and assisting LEEP users with various technical problems. LEEP Help Desk personnel also assist LEEP general users in changing passwords and providing security awareness training, if necessary.

Within the privileged user group, system administrators have the greatest access of all users. LEO system administrators ensure the availability and proper functioning of the LEO system. System administrators within LEO perform functions such as system installation, configuration, and management of all applications and servers which make up LEO. Database administrators install, configure, and manage the databases which support the SIG and VCC applications.

User groups other than general, privileged, and administrator exist to support the law enforcement entities represented within LEO membership. These groups are created with roles and permissions that restrict access and provide the minimal permissions to perform their specified duties. Examples of such groups include, but are not limited to, auditors, application developers, and system

testers.

All users must electronically acknowledge the LEEP Rules of Behavior before being granted access to LEO. LEO consists of criminal justice tools for authorized use only. As such, information on the @leo.gov email system, SIGs, and VCCs is to be used solely for criminal justice or other official business purposes of authorized users. By design, the range of authorized purposes for use of LEO is extremely broad. For example, two local police detectives may use the email system to arrange the time and place of a meeting regarding a robbery case and may include any or all types of PII in LEO email regarding suspects or witnesses. Furthermore, intelligence analysts may post reports in a SIG in order to share the information with all members.

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 LEO for open data purposes or for research or statistical analysis purposes. Only authorized users, as discussed above, have access to information in LEO.

Section 5: Notice, Consent, Access, and Amendment

5.1 ***What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.***

All individuals applying for a LEEP ID account receive a Privacy Act notice on their application. Once logged in to LEEP, all users can access the Privacy Statement linked at the bottom of the home page, which informs users about the information LEEP collects about its users and how the information is used. Similarly, the SIG and VCC homepages link to the Privacy Policy, which discusses the collection and use of information within LEO.

When logging in to LEEP, users also agree to a system use banner informing them they have no reasonable expectation of privacy regarding their activities on the system and any data transiting or stored on the system may be monitored, intercepted, searched and/or seized.

Within LEO, users may share information about non-LEO users who generally do not receive notice that their information is being shared. Non-LEO user information is collected, shared and utilized for criminal justice and other official purposes in accordance with federal and state laws and the LEO Terms and Conditions for Use. This privacy impact assessment and the system of records notices discussed in Section 7 provide general notice of the type of information shared within LEO.

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.

LEO users voluntarily log in to and use LEO applications (e.g., SIGs and VCCs). By using LEO, users consent to the collection and use of their information.

LEO users collect and share information about non-LEO users within LEO as part of their criminal justice, law enforcement, public safety, and national security missions. LEO users generally collect information shared within LEO in connection with law enforcement, public safety, and national security investigations; consequently, individuals generally do not have the opportunity to object to the collection of this information by the LEO users or to the sharing and retention of the information in LEO. Likewise, individuals generally do not have the opportunity to consent to particular uses of the information since it is obtained incident to criminal justice, public safety, and national security processes.

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.

LEO users can view and update their information through their LEEP profile or by contacting the LEEP Help desk.

Generally, non-LEO users do not have the ability to access or amend information in LEO. LEO users share information in LEO for criminal justice, public safety, and national security purposes. Allowing individuals to access information collected and used for these purposes could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of the FBI and other LEO users or interfere with the overall law enforcement process. Amendment of these records could similarly interfere with ongoing investigations and other activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised. LEO users are responsible for the accuracy, timeliness, and relevance of the records they share within LEO. SIG moderators and VCC administrators control the information within their SIGs and VCCs and may update or remove any information they determine is inaccurate, irrelevant, or stale.

The FBI has published Privacy Act exemptions for access and amendment rights for information in LEO. However, individuals may request access to their records by following the guidance provided on the FBI's website at https://www.fbi.gov/how-we-can-help-you/need-an-fbi-service-or-more-information/freedom-of-informationprivacy-act. 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/how-we-can-help-you/need-an-fbi-service-or-more-information/freedom-of-informationprivacy-act/requesting-fbi-records. The request should include a general description of the records sought, and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity, which can be located at the above link. In the initial request, the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search.

The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request. A determination of whether a record may be accessed will be made after a request is received.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** A three-year Authority to Operate was granted on October 31, 2019, and expires on November 9, 2022. A new ATO is expected in 2022 for the refactored LEO Amazon Web Services system before the expiration of the ATO on the current system. **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 security controls applied to LEO are commensurate with the potential impact on the organizational operations, organizational assets, and individuals should there be a loss of confidentiality, integrity, or availability.
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** As an FBI information system, LEO is required to perform a formal ATO Security Assessment and Authorization (SAA) derived from tailored requirements based on Federal Information Processing Standards 199 Categorization. This assessment requires that all applicable controls are addressed to ensure operational compliance within applicable NIST SP 800-53 and FBI policy. The last SAA was performed on 10/31/2019 granting a 3-year ATO which expires on 11/9/2022. To maintain ATO status, FBI information systems must undergo continuous monitoring which includes monthly vulnerability scanning and security control assessments on a quarterly basis at minimum.
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:** Audit logs capture information regarding what is accessed and modified. Auditing is performed to determine who accessed which information within LEO. Audit log Targets of Evaluation (ToE) for the LEO system are determined by the Security and Privacy Framework for FBI Information Systems security control AU-2. The audit logging ToE, frequency, and procedures are documented in the Audit Logging Management Plan. 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:** General information security training, including provisions regarding handling PII. Privileged User Training (Privileged Users), Incident Response Training (some Privileged Users), Contingency Plan Training (some Privileged Users), Rules of Behavior, Privacy Training (FBI Employees).

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?

LEO, as a U.S. Government Information System, adheres to FBI Security Assessment and Authorization and is subject to the Federal Information Security Modernization Act (FISMA) of 2014 to secure the Information System from unauthorized access and meet technical, management, and operational compliance with National Institute of Standards and Technology (NIST) SP 800-53 Security Controls. Access Control enforcement is inherited from LEEP as the trust center of gravity for the LEEP Federation. The Security Assessment and Authorization process is integrated into the life-cycle of an information system. The process serves as quality control for system security, ensuring the identification and integration of security related features and procedures which are implemented to provide the needed level of security. Security Assessment and Authorization processes provide for continuous monitoring, evaluation, and reviews of the implemented security controls for the identified information systems. The security assessment process provides for the evaluation and implementation of technical and nontechnical security features and safeguards that are used to meet the specified set of security requirements.

All users are required to be vetted, authorized, and authenticated through LEEP to access LEO. Once authenticated, access to the system is limited based on a user's role. Information is encrypted in transit and at rest. Access to information is audited and reviewed by the LEO System Administrators regularly, SSA daily, and the ISSO every 7 days. Before accessing LEEP and LEO, users must acknowledge the LEEP Rules of Behavior, including the Privacy and Security Statement, which informs users of the appropriate uses and sharing of LEO information and holds users accountable for the intentional or accidental misuse of information. Users are required to take annual FBI CJIS Division Information Spillage training as a supplement to Incident Response (IR) Training to further mitigate any unintentional information disclosure. This training aligns with FBI policy which establishes minimum actions required when responding to information spillage incidents. Additional information spillage training occurs within annual Information Security (INFOSEC) Awareness

training for all FBI information system users.

Audit controls are implemented to monitor staff and contractor use of user PII, including system monitoring tools and daily printed reports. Audited activities include the success and failure of logins, failure of attempts to use "privileged user" privileges, success or failure of attempts to grant any user privileges, and success or failure of attempts to change users' formal access permissions. LEO maintains near real-time monitoring of authorized and unauthorized activity. If suspicious activity is noted from monitoring alarms and alerts, the captured logs are reviewed by system and security personnel. This reduces the risk of unauthorized access and disclosure.

LEO is transitioning to a cloud environment. When transitioned, LEO 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 TLS FIPS 140-2 encryption, and all interconnections between the AWS GovCloud and the FBI utilize firewalls and security filtering. LEO 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 accounts and information in SIGs are destroyed six years after termination unless needed for investigative purposes. Retention periods for other types of information are included in National Archives and Records Administration (NARA)-approved retention schedule(s) or other records management requirements applicable to the record owning agency. See NARA Job Number N1-065-06-001. Each time a user accesses any of LEO's information-sharing applications, the system stores the data for specified periods of time as approved by the NARA retention schedule.

Once the event for which the VCC is opened has been resolved, the VCC administrator closes the VCC. VCC administrators can download their VCCs to Excel or a .pdf file. User agencies are responsible for maintaining their own policies and procedures on how the downloaded data is handled.

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.***

Sharing information in LEO creates privacy risks of unauthorized intentional access and disclosure of information, as well as unauthorized unintentional access and disclosure of information. Due to the flexibility of its applications, the types of information users can enter into LEO are potentially limitless. The human element plays a significant role concerning privacy risks, and measures to mitigate these risks include system access controls, annual information security awareness training for all users, privacy training for all FBI employees, and sweeping system audit controls. In addition, all LEO users are required to comply with the Terms and Conditions for Use.

Only authorized users can access LEO. As discussed in Section 4, authorized users are primarily members of the criminal justice, public safety, and national security communities. Private sector access to LEO is restricted to individuals with a demonstrated need for access. All private sector individuals must be sponsored by an authorized FBI LEEP user who certifies that the private sector individual has a need to access LEEP. The FBI reviews private sector accounts on an annual basis to ensure the individual still has a need to access LEEP. This reduces the risk of unauthorized access. LEO depends on its users to properly maintain the privacy of PII transmitted through the system in accordance with the LEEP Rules of Behavior, LEO Terms and Conditions of Use, and other federal regulations.

Privacy risks in the contexts of user PII and nonuser PII are mitigated by system access controls, annual information security awareness training, privacy training for FBI employees, and system audit controls. Users must complete security awareness training annually and must agree to the LEEP Rules of Behavior prior to being given access. If a user is found to have violated policy to a degree that is not serious enough to merit denying the user all future access, the user is briefed on his

responsibility and the user is re-administered the LEEP Rules of Behavior. All web-based access to LEO is secure and encrypted, accessible only to users with appropriate authorization and permissions. In addition, all users agree they will use LEEP and LEO for official business only and will limit distribution of information contained on LEO only to persons with a need to know.

Regarding nonuser related information in LEO, such as the content of emails, VCCs, and SIGs, (which include PII), two risks were identified: (1) LEO users could gain unauthorized access to this information (internal risk); and (2) nonusers could also gain access to this information (external risk). To mitigate the internal risk, LEO segregates information available to all users from information available to subject-specific users and requires specific authorization to access information only intended for subject-specific user audiences. Also, LEO users do not see other member information, except when those users are members of a community within which identities would be shared.

To mitigate the external risk, information from LEO is secure and encrypted while in transit, and access to LEO is provided only to users who have successfully authenticated through the LEEP federation. LEO incorporates a number of software applications to ensure data and software integrity and requires strict compliance with FBI security policy. LEO restricts access to many parts of the system, such as restricted and private SIGs. Access to VCCs is restricted by the VCC administrators. LEO maintains an audit log and informs all users they are subject to having their system activities monitored and recorded. LEO strictly adheres to the established *LEEP Procedure and Operations Manual* guidance for user access, the *FBI Security Policy*, *FBI CJIS Security Policy*, and *FBI Corporate Policy*. The *FBI CJIS Security Policy* provides information technology security requirements determined acceptable for the transmission, processing, and storage of CJIS Division data. Foreign user access to LEEP is limited to non-U.S. citizens with a demonstrated need for access. All foreign users with a LEEP ID account must be sponsored by an authorized LEEP user (either an FBI employee or a U.S. agency employing the foreign user) who certifies that the foreign user has a need to access LEEP. Foreign users accessing LEEP through an approved IdP are vetted by the IdP prior to receiving access to LEEP.[5]

The FBI anticipates criminal history information and other sensitive PII will be included in @leo.gov emails. Email is transmitted through email clients and servers over the Internet. If the recipient email domain supports TLS connections, LEO establishes a TLS connection with the recipient domain to ensure that the information (emails) is transmitted through an encrypted session. If, however, the recipient domain does not support TLS connections, the information (emails) is sent in clear text to the recipient domain. @leo.gov email also supports incoming TLS connections for those originating email services which support outgoing TLS connections. Emails containing PII (including criminal history and biometric information) are not differentiated from other emails. This poses a risk of an email containing PII being sent to members without a need to know and to nonmembers by accidentally typing an incorrect email address or intentionally causing a PII breach. The LEO Terms and Conditions for Use restrict the use of @leo.gov email to official business purposes. In addition, the Terms and Conditions for Use inform users that email is not necessarily secure, and users should consider other means of transmitting very sensitive information. All @leo.gov email traffic is logged and monitored for malicious content, fake actor accounts, and other

[5] Foreign user access to FBI information systems is addressed in FBI policy. In 2020, the FBI Chief Information Officer (CIO), the DOJ CIO, and the DOJ Department Security Officer granted LEO an exemption to allow foreign user access. The FBI and DOJ review the exemption annually.

security vulnerabilities.

The possibility that PII will be misused is generally increased by the number of people with access to it. Specifically, user PII is accessible to SIG moderators, VCC administrators and other privileged users via the administrative interfaces of the SIG and VCC applications. To mitigate privacy risks of making user PII available, required PII listed in the administrative interfaces of the SIG and VCC applications is limited to name, work telephone number, and work address.

LEO users can contact the LEEP Help Desk to access and redress issues with elements of their own information. Before any information is disclosed or updated, the LEEP Help Desk verifies the user's identity by asking the user for information from their application (such as name, last four (4) digits of their social security number, and a user-provided code word), as well as answers to user-provided security questions. Furthermore, the LEEP Help Desk verifies some descriptive data, such as employer information and agency POC, through an official employer representative before any updates are made.

Audit controls are implemented to monitor staff and contractor use of user PII, including system monitoring tools and daily printed reports. Audited activities include the success and failure of logins, failure of attempts to use "privileged user" privileges, success or failure of attempts to grant any user privileges, and success or failure of attempts to change users' formal access permissions. LEO maintains near real-time monitoring of authorized and unauthorized activity. If suspicious activity is noted from monitoring alarms and alerts, the captured logs are reviewed by system and security personnel. This reduces the risk of unauthorized access and data breaches.