Federal Bureau of Investigation

Privacy Impact Assessment
for the
Law Enforcement Online (LEO) Services

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

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: July 16, 2019

EXECUTIVE SUMMARY

Law Enforcement Online (LEO) Services 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 Controlled Unclassified Information (CUI) communication and information sharing for local, state, tribal, federal, foreign, 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 Services supports antiterrorism, intelligence, law enforcement, criminal justice, and public safety communities on a national and international level by providing and maintaining a secure communications network and provides a platform for online information sharing both internal and external to LEO Services.

This LEO Services Privacy Impact Assessment (PIA) is being conducted because LEO Services provides an information-sharing platform and collaboration site, which maintains and disseminates criminal justice and national security information including Personally Identifiable Information (PII) such as names, Social Security Numbers (SSNs), biometrics, financial account information, and medical information.

Section 1: Description of the Information System

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

This PIA is for Online Services and Operations Unit (OSOU) LEO Services, which is owned by the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division. The FBI CJIS Division Global Law Enforcement Support Section is charged with the development, operation, maintenance, and enhancement of the LEO Services network.

LEO Services 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 local, state, tribal, federal, foreign, 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 Services 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 Services provides a platform for online information sharing both internal and external to LEO Services.

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

LEO Services is a system that contains three separate services (each with its own icon): Special Interest Groups (SIGs), Virtual Command Centers (VCCs), and @leo.gov email. The icons are posted on the FBI's Law Enforcement Enterprise Portal (LEEP), which is a gateway for authorized LEEP federation users to access multiple systems and services by using single sign-

on technology.[1] Vetted and authorized users access LEO Services via industry-standard personal computers, laptops, tablets and smart phones through the LEEP federation identity providers (IdPs).[2]

The LEO Services platform consists of a number of different applications, such as information sharing platforms (SIGs), email, forums, alerts, calendars, and crisis management services (VCCs) available to all LEEP federation members. LEO Services members may use their LEO Services email accounts to send email to other LEO Services members or to share information externally with non-LEO Services email accounts. Forums are virtual bulletin boards on which LEO Services users may post information or questions for all other LEO Services users to see. Alerts provide the capability to broadcast messages to users of LEO Services. Shared information may include documents, articles, law enforcement forms, spreadsheets, presentations, images, and any other shared files made available to LEO Services users by other LEO Services users, for either online viewing or downloading.

The LEO Listservs, crisis management services, and National Alert System (NAS) are available through the SIG and VCC applications. A listserv is a mailing list that allows members to easily reach everyone subscribed to the listserv. Listservs are created with each SIG and VCC and can also be requested outside of these applications. Listserv messages are delivered by moderators or with a moderator's approval.

The NAS provides the capability to send one-way email messages to groups of users. NAS is an application accessible through both SIGs and VCCs by those users whose physical address is in the United States. SIG moderators and VCC administrators can activate the NAS for their respective SIG or VCC. Once activated, the NAS sends a one-way message from the SIGs/VCCs to the associated members of the SIGs/VCCs who have provided email addresses in their NAS user profile or to an ad hoc list of email addresses that is supplied by the moderator/administrator.

Louisiana State University (LSU) personnel run the LEEP Help Desk, located in Baton Rouge, Louisiana, which includes the LEEP Help Desk, Content Team, and Membership Team. The LEEP Help Desk provides end-user support to the LEO Services user community, membership services, and content design.

Each time a LEO Services user accesses any of LEO Services' information-sharing applications, LEO Services stores user-provided data for specified periods of time as approved by the National Archives and Records Administration (NARA) retention schedule. The content of the data shared via LEO Services' applications varies widely depending on the purposes for which it is

---

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

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

shared. For example, a LEO Services 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 Services' content, which is accessible to users for viewing, printing, or downloading, includes documents, spreadsheets, presentations, images, and other files.

Special Interest Groups (SIGs)

A SIG is a web-based, controlled-access area—an information-sharing platform created for departments, agencies, and specialized organizations to facilitate and enhance strategic collaboration among the criminal justice, national security, and public safety communities.

LEO Services 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's role is to manage the web space (SIG) within LEO Services. Each moderator chooses whether and/or how to share certain information with SIG members; this is not mandated by the FBI. For example, the Bomb Tech SIG will not share technical bulletins with nontechnical personnel.

The type of information contained within a SIG is determined by the users' needs. 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.

All content for SIGs is sent by SIG moderators to <content@leo.gov>, where it is passed through a classified information word filter scan. Content caught by the filter is placed into quarantine so FBI employees can review the documents to determine whether the content actually is classified. If the content is not classified, it is passed to the content team to be posted. If the content is classified, a spill incident has occurred and the incident response plan is activated. The Content Team does not alter the content of original shared documents. Once the content successfully passes through the filter, the Content Team posts the content within the appropriate SIG.

Virtual Command Center (VCC)

LEO Services also hosts the VCC application that provides timely situational control information to assist criminal justice, national security, intelligence, and public safety authorities with coordinating responses to crisis situations. The VCC contains readily available reference materials which are appropriate to particular events, venues, or interagency information sharing.

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 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 Services users with access to the 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 type 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. All VCCs are either restricted or private.

Once a VCC is no longer required for a specific event, the VCC must be closed by users with administrative privileges to the VCC. Information from the Events Board and static data posted to the VCC may be downloaded to Excel or saved as a .pdf document by the VCC Administrator through self-guided dropdown menus from the VCC dashboard.

@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.

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

LEO Services 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 Services is extremely broad and the information involved is likewise extremely broad. Users are able to include all types of PII about themselves or third parties, including name, aliases, all types of personal identification numbers, Personally Identifiable Financial Information, name, gender, date and place of birth, age, country of origin, nationality, address, telephone numbers, email address, 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 LEO Services within 180 days, his/her email account becomes inactive and the individual's information is no longer searchable in the address book.

In addition, LEO Services accesses user PII to produce LEO Services user access and activity records to ensure that LEO Services is being used appropriately and by authorized users only. Access to all LEO Services 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 Services user making these changes is recorded in the audit logs. LEO Services 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.

(d) who has access to information in the system

LEO Services 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 Services such as SIGs and VCCs. 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. Within the privileged user group, system administrators have the greatest access of all users. LEO Services System Administrators ensure the availability and proper functioning of the LEO Services system. User groups other than general, privileged, and administrator exist to support the law enforcement entities represented within the LEO Services 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.

In general, access to the SIGs and VCCs in this system will only be afforded to users accessing the system through LEEP federation IdPs, or those who have been properly vetted through the FBI's LeepID IdP.

More specifically, access control is provided by LEEP, which provides a single sign-on gateway to LEO Services, as well as other FBI resources. All LEO Services users must have access to LEEP through their own agency's IdP or through a LeepID account.

All users (general and privileged) must electronically acknowledge the LEEP Rules of Behavior before being granted access to LEO Services. Further, LEO Services has system security constraints and procedures to control user access to restricted and private 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 Services. 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 Services. On a case-by-case basis, intelligence analysts working as contractors for FSLTT government agencies may be given access to LEEP and LEO Services. Active duty and civilian military personnel are eligible for access to LEEP and LEO Services. Soldiers in a reserve or National Guard status may be granted access to LEEP and LEO Services 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 Services. 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 Services. General users have access to all public SIGs.

Restricted and private SIG members are 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 by the SIG moderator, based on a need to know. 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.

"Privileged Users" have a heightened access to all SIGs based on their need to manage the entire system. Such users include: The LEEP Help Desk; OSOU; and LEO Services System Administrators. LEEP Help Desk staff are contract personnel who are 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.

"System Administrators" have authority within the LEO Services system to perform functions such as the installation, configuration, and management of all applications and servers which make up the LEO Services system.

"Database Administrators" have the responsibility for installation, configuration, and management of the databases which support the SIGs and VCCs applications.

In order to properly limit LEO Services access to criminal justice, military, governmental personnel, and active LEEP account holders who are deemed appropriate (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 LeepID Account application. LEEP accounts are only granted after the IdP or the OSOU membership team vets the individual to ensure he or she meets the LEEP membership criteria.

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

Users access LEO Services through the LEEP Federation. The LEO Services hosted applications are available through the Internet. Information in the system is retrieved by the end user based

on their granted permissions. Once logged into a SIG or VCC, users can search for and retrieve content using keywords.

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

LEO Services is a human to machine interface. Users with approved access manually enter data into the SIG and VCC applications. 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. Within the SIGs, only the moderator can request information be added to the SIG. As discussed above, all content for SIGs is sent by SIG moderators to content@leo.gov. Once the information passes through classified filters and is received by the LEO Content Team, the Content Team posts the content within the appropriate SIG.

LEO Services is available through LEEP, which is a web-based system. Authorized LEEP users log into LEEP and then access the LEO Services where they can view and download information from SIGs and VCCs. 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. Email is transmitted through email clients and servers over the Internet. If the recipient email domain supports TLS connections, LEO Services 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.

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

The SIGs and VCCs are web applications deployed to the LEO Services application servers. These applications can utilize other functions within LEO Services, such as the @leo.gov email, LEO Listservs, crisis management services, and NAS. The SIGs and VCCs may contain links providing access to the other internal LEO Services functions, other FBI applications that are available within LEEP, external secured systems, or websites available on the public Internet.

LEO Services uses the CJIS Division Enterprise Storage Area Network (ESAN) for all storage requirements. Backup support is provided by the Enterprise Backup Services (EBS). LEO Services leverages the Shared Enterprise Network (SEN) environment provided by the Communications Technology Unit (CTU) for network connectivity.

(h) whether it is a general support system, major application, or other type of system

LEO Services is a controlled access system, which is open to all LEEP federation users who meet the membership criteria of LEEP, which may include private sector individuals who collaborate with the FBI or its partners to enhance criminal justice, national security, and public safety. LEO Services is categorized as a major application.

Section 2: Information in the System

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

(Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration	X	Financial account	X
Taxpayer ID	X	Driver's license	X	Financial transaction	X
Employee ID	X	Passport	X	Patient ID	X
File/case ID	X	Credit card	X		
Other identifying numbers (specify): Federation ID, which is a unique alphanumeric identification assigned to users by the system. It is required for access. None of the information marked above is required to be placed in SIGs or VCCs; however, 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 type of information may be shared to assist participating agencies in performing their official duties.					

General personal data					
Name	X	Date of birth	X	Religion	X
Maiden name	X	Place of birth	X	Financial info	X
Alias	X	Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service	X
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X	Education	X	Mother's maiden name	X
Other general personal data (specify): Country of Citizenship; LEO Services 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 type of information on non-LEO Services users may be shared within SIGs and VCCs to assist agencies in performing their official duties.					

Work-related data					
Occupation	X	Telephone number	X	Salary	X
Job title	X	Email address	X	Work history	X
Work address	X	Business associates	X		

Work-related data
Other work-related data (specify): Sworn Law Enforcement information; Intelligence Analyst information; ORI# (originating agency identifier); LEO Services 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 type of information on non-LEO Services users may be shared within SIGs and VCCs to assist agencies in performing their official duties.

Distinguishing features/Biometrics					
Fingerprints	X	Photos	X	DNA profiles	X
Palm prints	X	Scars, marks, tattoos	X	Retina/iris scans	X
Voice recording/signatures	X	Vascular scan	X	Dental profile	X
Other distinguishing features/biometrics (specify): LEO Services 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 type of information on non-LEO Services users may be shared within SIGs and VCCs to assist agencies in performing their official duties. However, LEO Services 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).					

The information above has the potential to be posted within an agency SIG or VCC.

A Rules of Behavior document is acknowledged through LEEP before any member can access the system. LEO Services consists of criminal justice tools for authorized use only. As such, information on the @leo.gov email system, SIGs, VCCs, and NASs 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 Services 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 Services email regarding suspects or witnesses. Furthermore, intelligence analysts may post reports in a SIG in order to share the information with all members.

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

Other information (specify)

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

Directly from individual about whom the information pertains					
In person	X	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	X	Public media, internet	X	Private sector	X
Commercial data brokers	X				
Other (specify):					

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.)

Regarding nonuser related information in LEO Services, such as the content of email, VCCs, and SIGs, (which include PII), two risks were identified: (1) LEO Services 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 Services 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 Services 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 Services is secure and encrypted while in transit, and access to LEO Services is provided only to users who have successfully authenticated through the LEEP federation. LEO Services incorporates a number of software applications to ensure data and software integrity, and requires strict compliance with FBI

security policy, which LEEP follows. LEO Services restricts access to many parts of the system, such as restricted and private SIGs. Access to VCCs is restricted by the VCC administrators. LEO Services maintains an audit log and informs all users they are subject to having all their system activities monitored and recorded. The LEO Services system 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 LeepID 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.[3]

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	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
X	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
	Other (specify):		

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.

LEO Services uses the personal information collected from LEEP users to determine the user's permission to access LEO Services and role. The particular user information is being collected to satisfy the shared mission of the LEO Services program, LEEP federation, the CJIS Division, and the FBI, which is to provide timely and relevant law enforcement assistance to its federal, state, local, tribal and international mission partners. LEO Services users' PII is permanently

[3] Foreign user access to FBI information systems is addressed in FBI Policy 0607D, Section 8.3. LEO was granted an informal exemption from FBI Policy 0261D in 2011, which 0607D superseded in 2013. A formal DOJ exemption for foreign user access is being pursued.

retained in the Access Management System (AMS) software application. The limited PII associated with the user access and activity while using LEO Services is stored in AMS for the purpose of granting access according to the users' permissions and maintaining an audit log of activity within LEO Services.

LEO Services users also share information through the @leo.gov email, SIGs and VCCs. The types of information shared through these emails, SIGs, and VCCs vary widely, and can include all types of PII. LEO Services consists of criminal justice tools for authorized use only. As such, information on VCCs and SIGs is to be used solely for criminal justice, national security, public safety, or other official business purposes. By design, the range of authorized purposes for use of SIGs, VCCs, and email is extremely broad. For example, VCCs provide tactical incident management support to law enforcement agencies and have been used in kidnappings, natural disasters, and active shooter events. VCC storage data could consist of Be On the Lookout alerts, advisories, threat assessments, manuals, operational guides, case summaries, and relevant photos. Two local police detectives may use the @leo.gov email system to arrange the time and place of a meeting regarding a robbery case and may include witness information. A state police officer may post a question on a SIG forum asking if other SIG members have experience applying for a certain kind of search warrant. FBI Intelligence analysts may post unclassified versions of FBI counterintelligence, criminal, and cyber intelligence reports for law enforcement information sharing purposes.

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 USC Chapter 33; 40 USC 1441 note; 44 USC 3101; 42 U.S.C. § 3771
	Executive Order	
X	Federal Regulation	28 CFR 0.85; 28 CFR Part 20
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

User accounts and information in SIGs are to be destroyed six years after termination unless needed for investigative purposes. Retention periods for other types of information are included in a NARA-approved retention schedule(s) or other records management requirements applicable

to the record owning agency. See NARA Job Number N1-065-06-1. Each time a user accesses any of LEO Services' 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 have the ability to 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.

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

PII Confidentiality Risk Level: ☐ **Low** ☐ **Moderate** ☑ **High**

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

☐ **Yes** ☑ **No**

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

Access controls

X	Access Enforcement: the system employs role-based access controls.
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 restrictions.
X	Access Control for Mobile Devices: Federated IdPs permit access to authorized users

	through mobile devices. LEO Services does not posture check the USER device. If a user accesses LEEP via agency owned mobile assets/devices, the device is controlled at the agency level. LEEP and LEO Services allow users to access the system from any public internet service provider on any internet capable device.

Audit controls

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

Identification and Authentication controls

X	Identification and Authentication: users are uniquely identified before accessing PII. Identification and authorization controls are inherited from LEEP.

Media controls

X	Media Access: access to system media (CDs, USB flash drives, backup tapes) is restricted.
X	Media Marking: media containing PII is labeled.
X	Media Storage: media containing PII is securely stored.
X	Media Transport: media is encrypted and stored in a locked container during transport.
X	Media Sanitation: media is sanitized prior to re-use
Media controls are inherited from Enterprise Storage Services (ESS)/Enterprise Storage Area Network (ESAN).	

Data Confidentiality controls

X	Transmission Confidentiality: Email is not always encrypted. If the destination email service support TLS connections, Leo Services email is sent via Secure Socket Layer (SSL)/TLS. If the destination does not support TLS, email is sent unencrypted over the network.
X	Protection of Information at Rest: LEO Services 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

Access to LEO Services is contingent upon LEEP membership and therefore restricted to individuals affiliated with the criminal justice system, intelligence communities, military personnel, governmental agencies associated with infrastructure protection of the United States, other individuals offering direct support to the criminal justice system, and select individuals from the private sector who collaborate with the FBI or its partners to enhance criminal justice,

national security, and public safety missions. All LEO Services users access LEO Services through an authorized LEEP federation IdP. An IdP is defined as an organization/agency which creates, maintains, and vets information about each of its authorized users for LEEP access. The IdP also assigns the current attributes about the individual for a given information technology session. These attributes are presented when the user accesses LEEP via a secure web browser session at a designated URL, which then allows the user access to LEO Services. LEEP performs user authentication each time an individual logs into LEEP. Private sector user access to LEEP and LEO Services 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. 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. All IdPs are required to review their users on an annual basis to ensure their users still meet LEEP membership criteria.

Documentation, training, and audit controls are in place to ensure the applicant information is appropriately handled. Standard Operating Procedures, System Administration Manuals, User Manuals, Privacy Act Statements, Agreement Forms, and System Security Plans are available to LEO Services staff. Training – including security awareness, Rules of Behavior, conferences, team meetings, and LEO Services published alerts – are provided to LEO Services staff to increase the adherence to appropriate privacy practices and policies.

LEO Services users are required to agree to the LEEP Rules of Behavior before accessing LEEP and once per year thereafter. All users must agree to the LEEP Rules of Behavior before accessing LEEP and adhere to the LEO Services Terms and Conditions for Use. Failure to abide by the LEEP Rules of Behavior and the LEO Services Terms and Conditions for Use may result in the termination of a user's LEEP account and access to LEO Services. Privileged users are required to take annual training on contingency planning, incident response, data spill management, and information security. General FBI users are required to take information security training annually. Non-FBI users are required to abide by the training requirements set forth in the CJIS Security Policy.

Audit controls are also 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 Services maintains near real-time monitoring of authorized and unauthorized activity. Such monitoring is performed by software applications and manual review. If suspicious activity is noted from monitoring alarms and alerts, the captured logs are reviewed by system and security personnel.

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		X	
DOJ components	X		X	
Federal entities	X		X	
State, local, tribal gov't entities	X		X	
Public	X			
Private sector	X		X	As discussed above, LEO Services 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 Services users may share information from LEO Services with non-LEO Services users for criminal justice or other official business purposes.
Foreign governments	X		X	As discussed above, LEO Services 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				
Other (specify):	X			On a case-by-case basis, LEO Services users may share information from LEO Services with non-LEO Services users for criminal justice or other official business purposes.

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.]

The Privacy risks identified in the sharing of information are the 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 Services 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 Services users are required to comply with the Terms and Conditions for Use.

As discussed above, private sector access to LEO Services 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 Services depends on its users to properly maintain the privacy of PII transmitted through the system in accordance with the LEEP Rules of Behavior 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 are given 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 Services is secure and encrypted, accessible only to users with appropriate authorization and permissions. In addition all users agree they will use LEEP and LEO Services for official business only and limit distribution of information contained on LEO Services only to persons with a need to know.

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 to so many authorized individuals, required PII listed in the administrative interfaces of the SIG and VCC applications is limited to name, work telephone number, and work address.

LEO Services users can also enlist the assistance of 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.

The FBI anticipates criminal history information and other Sensitive But Unclassified (SBU) PII will be found in @leo.gov emails. Emails containing PII (including criminal history and biometric information such as DNA data) 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 Services Terms and Conditions for Use restricts the use of @leo.gov email to official business purposes. In addition, the Terms and Conditions for Use informs 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 security vulnerabilities.

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 Services 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.

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: Acknowledging the LEEP Rules of Behavior. In addition, privacy and security statements are linked at the bottom of the LEEP home page and the SIG and VCC home pages. When logging into 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.
	No, notice is not provided.	Specify why not: Non-LEO Services users will not

X		have the opportunity to consent to particular uses of their information. The information is collected, shared and utilized for criminal justice and other official purposes in accordance with federal and state laws and the LEO Services Terms and Conditions for Use.

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

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: Through the LEEP application process.
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Individuals whose information is stored in applications such as VCCs and SIGs do not have an opportunity to decline to provide information because their access to LEO Services is dependent on collection of their information. In addition, individuals whose PII is entered into LEO Services by users have no opportunity to decline because the PII may be derived from an encounter with law enforcement or national security personnel.

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 are not given access if the required information is not provided. In addition, individuals whose PII is entered into LEO Services by users have no opportunity to consent to uses because that PII may be derived from an encounter with law enforcement or national security personnel.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these

principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Agreements concerning the security and privacy of the data are described in the LEEP membership application documents. Other agreements regarding security and privacy, such as the Privacy and Security Statement, exist in the form of system banners and system notices on LEEP and within the LEO Services, particularly SIGs and VCCs. System banners appear when users access the World Wide Web (WWW) connection site and at the LEEP user login page. To proceed past these system banners, users must click on an icon which states "Agree." The system banners disclose general information concerning security and privacy. The WWW connection site system banner reads:

> **WARNING!** You are accessing a U.S. Government information system, which includes this computer, this computer network, all computers connected to this network, and all devices and/or storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties. By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transiting or stored on this information system. Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

The LEO Services Privacy and Security Statement provides notice of LEO Services Terms and Conditions for Use, including general conduct; dissemination of information; information collected and stored automatically; information collected from email; security, intrusion, and detection; Privacy Statement; and other information and disclaimers.

Accessing LEO Services is strictly voluntary. By accessing LEO Services via LEEP, individuals providing PII via the access process agree to uses of their data which are necessary for the management of the system. They also agree to specific provisions which are contained in the Rules of Behavior by electronically acknowledging them through LEEP. Individual user's information must be provided to LEEP in order for LEEP to authenticate the user has permission to access LEEP and LEO Services. LeepID IdP provides the user notice as part of the application process in the form of a Privacy Act Statement on the connecting network. Users accessing LEEP through another IdP may receive notice from their IdP regarding how their information will be used and that it will be passed to LEEP. In addition, the LEEP homepage contains a link to the following notice:

> LEEP collects your user attributes (e.g. name, phone number, email address, and agency affiliation) from your identity provider. Your user attributes permit the

FBI to verify your identity and to confirm that you are qualified to be an authorized user of LEEP and its Service Providers. Your user attributes are passed to service providers accessible through LEEP for identity authentication purposes. Periodically identity providers will verify your user attributes to ensure you continue to meet account eligibility criteria.

LEEP will collect and store system and network related information in a persistent cookie. LEEP collects and stores this information to enhance its security by employing advanced authentication. LEEP will not share this information with any unauthorized parties.

Information in LEO Services may include PII on non-LEO Services users who do not have access to the system, and therefore, do not have an ability to control the use of their information within LEO Services or consent to the use of their information. The System of Records Notice covering LEO Services, the Notice of Proposed Rule Making to exempt this system from certain provisions of the Privacy Act under limited circumstances, and this Privacy Impact Assessment provide notice to non-LEO Services users that some information about them may be shared within LEO Services. Because LEO Services supports criminal justice, law enforcement, and national security purposes, it is not feasible to inform non-LEO Services users of the use of their PII within LEO Services. Data placed within the above applications is the sole responsibility of the user, not the LEO Services program.

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: Only vetted and authorized users are granted access to the system.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Audit logs capture information regarding what is accessed and modified. The logs are reviewed regularly for suspicious activity.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: A three year Authority to Operate was granted on October 31, 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: Auditing is performed to determine who accessed which responses within LEO Services.

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, including provisions regarding handling PII.
		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): 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 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.]

LEO Services, 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 800-54 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 to be 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 to access LEO Services through LEEP. Once authenticated, access to the system is limited based on a user's role. Information is sent encrypted. Access information is audited and reviewed by the system's staff. Before being awarded access, users are required to acknowledge the LEEP Rules of Behavior, including the Privacy and Security Statement, which makes users accountable for the intentional or accidental misuse of information. Users are required to take training to further mitigate any unintentional information disclosure.

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 Services 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.

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: JUSTICE/FBI-004, *FBI Online Collaboration Systems,* 82 Fed. Reg. 57291 (Dec. 4, 2017); DOJ-002, *Department of Justice Computer Systems Activity and Access Records*, 64 Fed. Reg. 73,585 (Dec. 30, 1999), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001) and 82 FR 24151 (May 25, 2017).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

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

Email addresses are retrieved by the name and/or email address of the user. Listserv address lists are organized by topic or the names of organizations. SIG information is retrieved by topic, location, and names of individuals. The VCC application is a tactical, real-time collaboration tool which facilitates shared situational awareness and incident management, including threat monitoring and live updates. The VCC is used to post information to authorized members. Information in SIGs and VCCs can be searched and retrieved by keyword.