Fax to: (877) 2 FAX LEO
(877) 232-9536
Law Enforcement Online
402 Johnston Hall
Baton Rouge, LA 70803
membership@leo.gov

Law Enforcement Online
LEO User Application

WARNING

LEO is an official U.S. Government system for authorized use only by authorized members of the law enforcement, criminal justice and public safety community. Information presented in this system is considered sensitive but not classified and is for official law enforcement/criminal justice/public safety use only. The use of this system will be monitored for security and administration purposes and accessing this system constitutes consent to such monitoring. Any unauthorized access of this system or unauthorized use of the information provided on the LEO network is prohibited and may be subject to criminal and civil penalties under federal law.

This FBI system is for the sole use of authorized users for official business only. You have no expectation of privacy in its use. To protect the system from unauthorized use and to insure that the system is functioning properly, individuals using this computer are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials.

LEO will collect and store system and network related information in a persistent cookie. The purpose of collecting and storing this information is so that LEO can enhance its security by employing advanced authentication reliant on this information. The information is encrypted and LEO will not share this with any unauthorized parties.

Warning! The use of publicly accessible computers (e.g. libraries, airports, cafes, hotels, etc.) to access LEO is unauthorized. This type of usage may result in the involuntary dissemination of information to unauthorized entities. Data may be left on this computer resulting in the next person using this machine the ability to view your data.

PRIVACY ACT STATEMENT

General - This information is provided pursuant to Public Law 93-579 (Privacy Act of 1974) for individuals completing LEO user application forms. Authority - LEO is a federally funded national communications system established by the FBI. Application information is solicited under the authority of the Federal Records Act (Title 44, United States Code) and implementing regulations (Title 36, Code of Federal Regulations, chapter XII). Purpose and Use - The principal purposes of LEO user application forms are to collect information needed to determine qualifying factors for authorized use, and verification of identity. This completed application will be used to register this account as a qualified LEO account. All or part of the submitted information may be disclosed outside the FBI to federal, state, local, or tribal law enforcement agencies charged with the responsibility of investigating a violation or potential violation of the law and to applicant agency or organization to periodically verify continued access to LEO. Disclosure may otherwise be made pursuant to the routine uses most recently published in the Federal Register for the FBI's Central Records System (Justice/FBI 002). Failure to provide the requested information shall result in the denial of this application.

Instructions: Type or write the information requested. **ALL FIELDS ARE MANDATORY**. Fax, mail, or e-mail the completed application to the information located in the upper right hand portion of page one of this form. **Send all pages, including a signed FD-889 Rules of Behavior form.** IMPORTANT: Non-legible applications will not be processed

1. Applicant Information

Applicant Name (Last, First, MI) :

Title / Position:
(do not abbreviate)

Email Address:

Are you a US citizen? Yes ◯ No ◯

Country of Citizenship, List all:

2. Applicant Security Verification Information

Social Security Number or Passport # if International:	Date of Birth:	Gender :	Code Word: (ex: Mother's Maiden Name)
- - Pursuant to executive order 9397 and used for employment verification		Male ◯ Female ◯	

Are you a Sworn Law Enforcement Officer (arresting powers)?
Yes ◯ No ◯
If Yes, Please enter ORI:

Do you want to share your LEO email address with HSIN, RISSNET, and INTELINK users?
Yes ◯ No ◯

Are you an Intelligence Analyst
Yes ◯ No ◯

Are you a UNet user? Yes ◯ No ◯
If yes, please enter email address:

3. Employing Agency / Organization Information

Agency / Org Name:

Agency / Jurisdiction: Local ◯ State ◯ Federal ◯ Tribal ◯ FBI Contractor ◯ Sponsored Applicant ◯ International User ◯

Agency / Org Type: Law Enforcement ◯ Military ◯ Emergency Management ◯ Government/Other ◯

Specify Government/Other:

Business Address:
(No P.O. Boxes)

Phone:

Alternate Phone:

If you are an FBI Contractor, Sponsored Applicant, or International User, sections 4, 5, and 6 must be completed.

4. Sponsoring Person Information

If you are an FBI Contractor, sponsoring person must be a current FBI employee with an active LEO account. If you are a Sponsored Applicant, sponsoring person must have an active LEO account. If you are an International User, sponsoring person must be an FBI Legal Attaché or FBI Assistant Legal Attaché.

Sponsoring person's Name (Last, First, MI):

Agency:

Title / Position:
(do not abbreviate)

Business Mailing Address: (no PO Boxes)	**Phone:**
	Alternate Phone:
	LEO E-mail:
	Alternate E-mail:

5. Name and Description of Project, Justification of Access

Project or Law Enforcement related work description:

Length of Access requested if membership is requested for a project or special event **From:** **To:**

Restricted Access if requested: LEO Email Only ☐ **Specific SIG only access** ☐ **- requires Moderator to complete section 6**

6. Sponsoring Person / Point of Contact Certification (Please complete signature lines)

I hereby certify that the above named individual is authorized to have access to the Law Enforcement Online (LEO) system. Additionally, I agree that I must re-certify access to LEO for the above named individual every six months.

X _____

SIGNATURE **MONTH / DAY / YEAR**

7. Optional Moderator's Information

Moderator's Name:

SIG's / VCC's Requested for LEO Applicant:

X _____

MODERATOR'S SIGNATURE **MONTH / DAY / YEAR**

FD-889 Revised 8-24-2009 Previous Versions Obsolete	FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form

Purpose: This agreement outlines the acceptable and unacceptable uses of FBI Information Technology (IT) and Information Systems (IS). It also outlines the signer's responsibilities regarding stewardship and use of FBI IT/IS and Public Key Infrastructure (PKI) assets and capabilities if a PKI token is issued.

Scope: This agreement applies to anyone granted access to any FBI IT/IS, including but not limited to: FBI employees, contractors, interns, detailees, and personnel from Other Government Agencies (e.g., Federal, state, municipal, or tribal). All references to IT/IS monitoring herein pertain to data communications only (emails, facsimile, computer database use and data storage, digital transmission of data, etc.) and not to voice communications. This agreement form must be signed before access to any FBI IT/IS is granted. To remain compliant with applicable statutes, orders, regulations, and directives, the FBI will update this form. It is your responsibility to maintain current knowledge of the FBI IT/IS Rules of Behavior for General Users.

References:

- Standards of Ethical Conduct Regulation (5 CFR Parts 2635 and 3801).
- The Federal Information Security Management Act (FISMA) of 2002.
- Corporate Policy Directive 0071D, FBI Information System Use Policy
- The FBI Security Policy Manual (SPM).
- FBI Manual of Investigative Operations and Guidelines (MIOG) Part II Section 16-18.
- FBI Manual of Administrative Operations and Procedures (MAOP) Part II Section 2-1.1 and Section 9-3.1.5.
- FBI Unclassified Network (UNet) Policy Version 1.0, 3 April, 2007
- U.S. Department of Justice (DOJ) Public Key Infrastructure X.509 Certificate Policy v1.13, 15 December, 2006.
- X.509 Certification Practices Statement for the Federal Bureau of Investigation High Assurance Certificate Authority v3.0, 31 October 2005.
- FD-1001 (1-22-2007) DOJ Consent For Warrantless Searches Of Department Of Justice Workplaces.
- US Code, Title 18, Section 798.
- The Privacy Act of 1974 (as amended) 5 USC 552a
- FD-291, FBI Employment Agreement
- FD-857, Sensitive Information Nondisclosure Agreement
- FD-868, Nondisclosure Agreement for Joint Task Force Members, Contractors, Detailees, Assignees, and Interns
- SF-312, Classified Information Nondisclosure Agreement
- Form 4414, Sensitive Compartmented Information Nondisclosure Agreement
- Office of Management and Budget (OMB) Circular A-130
- Department of Justice (DOJ) IT Security Standards
- Department of Justice (DOJ) 2740.1 series
- Internal Revenue Service Code, sections 7213 and 7213 A (USC 26, 7213).

Statement of Responsibility: I understand that I am to use FBI systems for lawful, official use and authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations) and as further outlined in this document and other FBI policy directives. Even where granted access, I must only access the system files and information on a need-to-know basis and only in furtherance of authorized tasks or mission related-functions.

FD-889 Revised 8-24-2009 Previous Versions Obsolete	FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form

General. I am responsible for all activity on any FBI IS that is authorized to operate in FBI space and that occurs on my individual account(s) once my logon credential or password has been used to logon. If I am a member of a "group account," I am responsible for all of my activity when I am logged on an IS associated with that account.

I am responsible for all IT that I introduce into FBI approved space including devices that are privately owned, or those owned by another government agency. I understand that I must obtain written permission to introduce any non-FBI hardware, software, or media into FBI controlled space, and that I may not use non-FBI hardware, software, or media to connect to or communicate with any FBI system without authorization from the Head of my Division and the Assistant Director for Security, or designee.

I acknowledge that the ultimate responsibility for ensuring the protection of FBI non-public information lies with me, the user of FBI IT/IS and non-FBI IT/IS authorized to operate in FBI spaces.

I acknowledge that I am prohibited from accessing or using FBI or Department of Justice information about other individuals, including tax information and personally identifiable information, except on a need-to-know basis in furtherance of authorized tasks or mission related-functions. I am obligated to maintain, process, and protect information about other individuals with sufficient care to ensure the security and confidentiality of the information and protect it from inadvertent or unauthorized disclosure. I am not permitted to disclose information about other individuals outside the Department of Justice except when authorized under the Privacy Act (5 USC 552a(b)).

Revocability: The ability to use IT in FBI space and access to FBI IT/IS is a revocable privilege.

Rules of Behavior: I will adhere to the following Rules of Behavior (ROB):

1. I consent to monitoring or search of any IT/IS equipment or media I bring into, or remove from, FBI owned, controlled or leased facilities. When asked by authorized personnel I will provide unfettered access to all equipment or media brought into or removed from such FBI facilities. I also understand that FBI or FBI leased IS may be monitored or otherwise accessed for law enforcement or other compliance purposes and my agreement to this FBI ROB constitutes my consent to be monitored and to allow access to FBI IS accessed by me.

2. The following applies **only** to personnel from Other Government Agencies whose duties require them to bring IT/IS assets (e.g., laptop or desktop computers) owned or leased by their parent agency into FBI facilities.

> I understand that the aforementioned IT/IS assets are also subject to FBI search and/or monitoring; however, prior to any search or monitoring the FBI will coordinate with the appropriate Security Personnel or other responsible representatives of my parent agency to afford my agency an opportunity to provide warnings to the FBI about the types of information that may exist within my IT/IS devices and to ensure that my agency is afforded the opportunity to have appropriate representation during any and all searches.

3. I will read, understand, and adhere to all FBI information assurance policy directives, including the FBI Security Policy Manual (SPM), Policy Directives of the FBI, MAOP, MIOG and local Standard Operating Procedures and I will address any questions regarding policy,

responsibilities, and duties to my Information System Security Officer (ISSO), Information System Security Manager (ISSM), or Chief Security Officer (CSO). I will:

a. Use only properly licensed FBI approved software and hardware.

b. Protect all copyright and other intellectual property rights according to terms and conditions contained in FBI approved software and hardware licenses.

c. Use FBI IT equipment, including but not limited to portable electronic devices (PED) and keyboard, video, monitor (KVM) switch devices, according to and in compliance with FBI policy directives.

d. Use FBI computer and network applications and systems, including but not limited to, email, databases, and web services according to and in compliance with FBI policy directives.

e. Use FBI embedded and add-on peripheral devices including cameras, microphones, and storage devices according to and in compliance with FBI policy directives.

4. I will read and understand the FBI standard information system (IS) and network warning banner that is presented prior to IS or network log on. I will address any questions regarding that banner to my Information System Security Officer (ISSO), Information System Security Manager (ISSM), or Chief Security Officer (CSO). I will:

a. Ensure that I understand and respect the accredited security level of FBI facilities and of FBI IT systems that I work with or access.

b. Operate FBI IT systems and technology processing classified information only in space that is approved for the highest classification level of the information contained on the IT system or technology. When not in use, I will store classified computers and hard-drives in an approved security container or in a facility approved for open storage of the information that the device or system contains.

c. Operate IT systems processing sensitive but unclassified information only in space approved for processing of that sensitive but unclassified information. When not in use, I will store sensitive unclassified computers and hard-drives according to FBI security policy for the information to which I have access.

d. Use FBI approved Cross Domain Data Transfer procedures for every transfer of information between FBI security domains.

5. When using FBI IT/IS, I will:

a. Use strong passwords as defined in the FBI SPM and Policy Directives of the FBI, and agree to change my password with a frequency as specified by policy or as requested for security reasons.

b. Protect my password(s) according to the classification level of the system or at the highest classification of the data being secured. I will protect my passwords from disclosure to other people.

c. Use screen locks or logoff my workstation upon departing the immediate area.

d. Use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.

e. Use only authorized media (thumb drives, diskettes, etc) and procedures to download or store FBI information.

f. Properly mark and label classified and sensitive information and media (removable and fixed) according to FBI policy, the Department of Justice Program Operating Manual, DOJ Order 2620.7, and the Director of National Intelligence (DNI) Controlled Access Program Coordination Office (CAPCO) guidelines, as appropriate.

g. Encrypt, using FBI approved solutions, all sensitive and classified data that is stored on portable electronic or optical media, and data stored on computers that are transported outside of FBI controlled spaces.

h. Disseminate any FBI non-public information only to persons who have a verified authorization to access the information and appropriate security clearance.

i. Destroy copies and extracts of sensitive data that are no longer needed using FBI approved destruction procedures.

6. While traveling on FBI business, I will minimize information on my accessible IT systems and components to exactly what is needed to perform my mission.

7. Prior to traveling overseas or to a foreign nation, I will attend to all required overseas travel briefings, as related to traveling with Information Technology or Information Systems.

8. I will complete the FBI's Annual INFOSEC Awareness Training or provide my ISSO, ISSM or CSO with adequate documentation of my completion of my employing agency's annual information security training.

9. If designated as a "*Privileged User*" I will complete the required Privileged User Security training and sign the *Privileged User* Rules of Behavior form.

10. I will immediately report known or suspected security incidents or improper use of FBI IT/IS to my CSO according to FBI Policy Directives upon discovery regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information according to the appropriate FBI incident response plan, and Security Incident Response System (SIRS) procedures.

11. ***If*** issued digital certificates by the FBI PKI Certification Authority (CA), in addition to the above I will:

a. Use the certificate and corresponding keys exclusively for authorized and legal purposes for which they are issued and only use key pairs bound to valid certificates. Note: Explanation of what certificates, keys, and key pairs are and how to use them is explained on the PKI Registration Form when the token is issued.

b. Re-authenticate my identity to the FBI CA in-person and register for certificate re-key at least once every three years, or as instructed by designated authorities.

c. Protect my token and private keys from unauthorized access and be aware of the location of my token and ensure its security at all times, whether in my immediate possession, in FBI space, or in my home.

d. Use strong passwords.

e. Immediately request my ISSO, ISSM, or CSO or an authorized FBI PKI authority to revoke my associated credentials if I suspect that my token or keys are lost/stolen or if my password was compromised.

Expressly Prohibited Behavior: I will ***NOT*** conduct or participate in any of the following behaviors or activities on any FBI IT, IS, or on other agency IT/IS systems authorized to operate in FBI space. Unless required as part of my official duties, I will not:

1. Knowingly violate any statute or order, such as compliance legislation, copyright laws, or laws governing disclosure of information, including but not limited to:

a. Attempt to process or enter information onto a system exceeding the authorized classification level for that IT/IS (e.g., placing Secret information on an Unclassified enclave).

b. Connect classified IT/IS to the Internet or other unclassified systems.

c. Remove sensitive/classified media (paper or electronic) from controlled areas/facilities (i.e. taking classified media home) without authorization.

d. Use FBI IT/IS or FBI non-public information for personal benefit, profit, to benefit other persons, non-profit business dealings, any political (e.g., lobbying or campaigning) party candidate or issue or for any illegal activity.

2. Misuse my FBI IT/IS privileges including:

a. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).

b. Permit any unauthorized person access to a government-owned or government-operated system, device, or service.

c. Use an account, user ID, or password not specifically assigned to me, masquerade as another user, or otherwise misrepresent my identity and privileges to IT/IS administrators and security personnel.

3. Exhibit behavior that could lead to damage, endangerment or degradation of FBI equipment, software, media, data, facilities, services, or people, including but not limited to:

a. Attempt to circumvent access controls or to use unauthorized means (e.g., penetration testing, password cracking, “sniffer” programs), to gain access to accounts, files, folders or data on FBI IT/IS.

b. Change configuration settings of operating systems or security related software, or security related information. Nor will I remove, modify, or add any hardware or software to/from FBI IT/IS without approval of my ISSO.

c. Tamper (e.g., alter, change, configure, install software or hardware, or connect IT or systems) with my computer to circumvent any FBI policy and IT/IS protections.

d. Open e-mails or other messages from suspicious sources (e.g., sources that you do not recognize as legitimate for your line of business).

e. Visit untrustworthy or inappropriate Web sites. For example, I will pay careful attention to the Universal Resource Locator (URL) of a web site inasmuch as URLs for malicious or untrustworthy web sites may look identical to a legitimate web site, but the URL may use a variation in spelling or a different domain (e.g., .com instead of net; or .com in place of .gov).

f. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).

g. Create or intentionally spread malicious code (i.e. viruses and Trojans).

h. Attempt to access any security audit trail information that may exist without authorization.

i. Install or connect non-FBI owned or leased (including privately owned) software or hardware (e.g., PEDS, such as Palm Pilots, Blackberrys, MP3 Players…etc.) and removable media (e.g., thumb drives, memory sticks…etc.) to FBI IT/IS.

j. Introduce wireless devices into FBI space without authorization from the ISSM.

4. Participate in prohibited activities, including but not limited to:

a. Download, view, or send pornography or obscene material.

b. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.

c. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional according to FBI standards of professional behavior.

d. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.

e. Use internet “chat” services (e.g., AOL, Instant Messenger (IM), Microsoft Network IM, Yahoo IM…etc).

f. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).

g. “Surf” through FBI files containing personal information merely for personal curiosity.

h. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.).

i. Use personal e-mail services (such as Yahoo, Gmail, etc.) for government business.

j. Download attachments via Outlook Web Access to a non-government computer.

Privacy Act Statement:
The information solicited on this form is collected pursuant to the Federal Information Security Management Act (FISMA) of 2002, the Computer Security Act of 1987, the general recordkeeping provision of the Administrative Procedures Act (5 U.S.C. § 301) and Executive Order 9397, as amended by Executive Order 13478, which permits (but does not require) the collection of social security numbers.

The Public Key Infrastructure (PKI) portion of this agreement is collected pursuant to 5 U.S.C. §§ 3301, 9101, Exec. Order No. 12968, Exec. Order No. 10450, and 28 C.F.R. § 0.138. Pursuant to the Privacy Act of 1974, 5 U.S.C. § 552a, we are providing the following information on principal purposes and routine uses.

The principal purpose of this form is to verify that individual signatories are aware of the rules of behavior that govern access to FBI IT/IS that operate in FBI space. If a digital certificate from the FBI PKI is issued, this form also supports the operation of the PKI Program, which is designed to increase the security posture of the FBI. For the PKI Program, the information submitted will be used to verify user identity in support of the digital signatures and data encryption/decryption provided by the FBI PKI system. This information, in conjunction with the PKI digital signatures and data encryption/decryption, is used to provide Authentication, Non-repudiation, and Confidentiality services.

The information on this form may be shared within the Department of Justice (DOJ) components and with other governmental agencies for the purpose of providing access to these facilities, facilitating information sharing (i.e., sending encrypted e-mails), and for other authorized purposes.

In addition, information may be disclosed to the following;

1. Appropriate federal, state, local, tribal, foreign or other public authorities conducting criminal, intelligence, or security background investigations.
2. Officials or employees of other federal agencies to assist in the performance of their duties when disclosure is compatible with the purposes for which the information was collected.
3. To contractors, grantees, experts, consultants, or others when necessary to accomplish an agency function.
4. Pursuant to applicable routine uses for the FBI's Central Records System (Justice/FBI-002), which is where the information solicited on this form will be maintained.

The provision of the information is voluntary, but without your acknowledgment of the rules of behavior for accessing FBI information, and IT/IS that operate in FBI space, you may not be permitted such access or receive FBI PKI credentials and certificates, which may affect your ability to perform your official duties. Disclosure of the last four digits of your social security number is also voluntary, but will help to differentiate you from other individuals with the same or a similar name.

FD-889 Revised 8-24-2009 Previous Versions Obsolete	FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form

Acknowledgment
I acknowledge that I have read and understand the above listed Rules of Behavior. I also state that I will adhere to these Rules of Behavior and that failure to do so may constitute a security violation resulting in denial of access to FBI IT/IS networks or facilities. I also understand that violation of these rules of behavior will be reported to the appropriate authorities and may result in administrative, criminal, or other adverse disciplinary action deemed appropriate

Printed Name: _____ Date: _____

Employee Signature: _____ Last Four of SSN: xxx-xx-_____

FBI Personnel File Number (if known): _____
Note: If applicable, other Govt. Agency (Federal, state, or municipality) _____

Filing Instructions: Completion of the FBI's annual INFOSEC Awareness Training satisfied the signatory and acknowledgement requirements for the purpose of storage and audit of this form. When a hardcopy is required, CSOs are responsible for filing this form IAW EC 319W-HQ-A1487698-SECD Serial 88 Form Owner: Career Services Management Unit and Information Assurance Section, FBI SecD.