LAW ENFORCEMENT ONLINE

Securely sign in to LEO here:

User ID: Password: Log In

VeriSign Secured

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.

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.*

LEO supports the FBI's ten priorities by providing cost-effective, time-critical national alerts and information sharing to public safety, law enforcement, antiterrorism and intelligence agencies in support of the Global War on Terrorism. LEO is provided to members of the law enforcement community at no cost to their respective agencies. It is the mission of LEO to catalyze and enhance collaboration and information exchange across the FBI and mission partners with state-of-the-art commercial off-the-shelf communications services and tools, providing a user-friendly portal and software for communications and information exchange.

LEO is a 7 days a week, 24 hours a day online (real-time), controlled-access communications and information sharing data repository. It provides an Internet accessible focal point for electronic Sensitive But Unclassified (SBU) communication and information sharing for the international, federal, state, local, and tribal law enforcement agencies. LEO also supports antiterrorism, intelligence, law enforcement, criminal justice, and public safety communities worldwide. Users anywhere in the world can communicate securely using LEO.

Click Here to View the LEO Membership Criteria

Click Here to Download the LEO User Application

National Alert System

The LEO National Alert System (NAS) is an alert system that can deliver secure information to 20,000 users/command centers within 5 minutes. The NAS is capable of sending up to 160,000 unsecured notifications to pagers, cellular phones, and other wireless devices to advise that an alert has been sent.

Virtual Command Center

The VCC is a situational awareness mechanism and crisis management tool that is used for tracking, displaying, and disseminating intelligence and tactical information. In addition, the VCC provides ready access to a wide range of reference materials that are appropriate to the event and/or venue. Because the VCC resides on the LEO system, it can be utilized and/or reviewed by authorized members from multiple, geographically dispersed locations.

N-DEx, OneDOJ, and LEO Access

The Law Enforcement National Data Exchange (N-DEx), the OneDOJ, and the Law Enforcement Online (LEO) are the FBI CJIS Division Services & Systems currently covered by the access forms you will be downloading. Access to the N-DEx during Increment 1 will be through the LEO, so both accounts must be established. When requesting access, be aware that N-DEx, OneDOJ, and LEO, are official U.S. Government systems for authorized use only by authorized members of the law enforcement, criminal justice, and public safety community. You must submit both the Access Request and Rules of Behavior to be processed.

Click here to select the appropriate access form.

LEO Support Center

- (888) 334-4LEO (4536)
- TTY: (304) 625-3963

LAW ENFORCEMENT ONLINE

Please Select an Application Below:

- LEO Regular User Application
- LEO Contractor Application
- LEO International Application

LEO Support Center

(888) 334-4LEO (4536)
TTY: (304) 625-3963

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

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**. When completed, fax or mail to the information provided 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 ○ Dual ○ **List all citizenships held other than US:**

2. Applicant Security Verification Information

Last 6 digits of SSN:	Date of Birth:	Code Word: (ex: Mother's Maiden Name)
XXX --		

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

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 (Eligibility: U.S., U.S. Territories, U.S. Possessions Only)

Agency / Org Name:

Agency / Org Jurisdiction: Local ○ State ○ Federal ○ Tribal ○

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

Specify Government/Other:

Address:
(No P.O. Boxes)

Phone:

Alternate Phone:

FD-889 Revised 12/05/08 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 does not apply to voice communications. This agreement form must be signed before access to any FBI IT/IS is granted.

References:

- Standards of Ethical Conduct Regulation (5 CFR Parts 2635 and 3801).
- The Federal Information Security Management Act (FISMA) of 2002.
- 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

Statement of Responsibility: I understand that I am to use FBI systems for lawful, official use and authorized purposes in accordance with current FBI guidelines. I am responsible for all IT that I introduce into FBI space including devices that are privately owned, or those owned by another government agency.

I am responsible for all activity on FBI IS's, as well as any other IT/IS's that are authorized to operate in FBI space, 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 activity when I am logged on an IS associated with that account.

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

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 I am prohibited from accessing or using information about individuals 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 individuals with sufficient care in order to ensure the security and confidentiality of the information and protect if from inadvertent or unauthorized disclosure. Even within the FBI and the Department of Justice, I am only permitted to disclose information about individuals on a need-to-know basis for performance of authorized tasks or mission related-functions. I am not permitted to disclose information about individuals outside the Department of Justice except when authorized under the Privacy Act (5 USC 552a(b)).

Access: Access to FBI IT, IS, networks, and other agency systems operating in FBI spaces is for official and authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations) (noted above) and as further outlined in this document.

Even where granted access, I must only access the system files and information on a need-to-know basis in furtherance of authorized tasks or mission related-functions.

Revocability: The ability to use IT in FBI space and access to FBI IS's is a revocable privilege. IT used in FBI space is subject to vulnerability assessment, content monitoring, activity monitoring, and security testing.

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's 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's accessed by me.
2. The following (2.a.) 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:
    a. 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.
4. I will comply with the FBI 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).
5. I will read and understand the FBI standard information system (IS) and network warning banner prior to logging onto the IS or network.

6. I will 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.
7. I will use FBI computer and network applications and systems, including but not limited to, e-mail, databases, and web services according to and in compliance with FBI policy directives.
8. I will ensure that I understand and respect the accredited security level of FBI facilities and of FBI IT systems that I work with or access.
9. I will protect my password(s) in accordance with the classification level of the system or at the highest classification of the data being secured.
10. I will only 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.
11. I will use screen locks or logoff my workstation upon departing the immediate area.
12. I will use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.
13. I will use only authorized media (thumb drives, diskettes, etc) and procedures to download FBI information.
14. I will 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 Coordination Office (CAPCO) guidelines, as appropriate.
15. I will 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.
16. When not in use, I will store classified computers in an approved security container, or in a facility approved for open storage of the information contained on that classified computer.
17. I will destroy copies and extracts of sensitive data that are no longer needed.
18. I will not disseminate any FBI non-public information to anyone who does not have a verified authorization to access the information and appropriate security clearance.
19. 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.
20. If designated as a "*Privileged User*" I will complete the required Privileged User Security training and sign the *Privileged User* Rules of Behavior form.
21. I will immediately report known or suspected security incidents or improper use to my ISSO, ISSM, or CSO according to SPM guidelines and FBI Policy Directives upon discovery regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information to the CSO according to the appropriate FBI incident response plan.
22. ***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 the "strong password" guidance mentioned in 4 and 5 above.

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.

23. 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.
24. 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.

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 authorize to operate in FBI space, unless required as part of my official duties:

1. Knowingly violate any statute or orders, such as compliance legislation, copyright laws or laws governing disclosure of information.
2. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).
3. 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.
4. Attempt to circumvent access controls or to use unauthorized means to gain access to accounts, files, folders or data on FBI IT/IS.
5. 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 from FBI IT without approval of my ISSO.
6. Permit any unauthorized individual access to a government-owned or government-operated system, device, or service.
7. Exhibit behaviors that could lead to damage, endangerment or degradation of FBI equipment, software, media, data, facilities, services, or people.
8. 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.
9. 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.
10. Connect classified IT or IS's to the Internet or other unclassified systems.
11. Attempt to process or enter information onto a system exceeding the authorized classification level. (e.g., placing Top Secret information on Secret Enclave).
12. Operate IT systems, whether fixed or portable, in areas or facilities that are not approved by the Assistant Director for Security for processing the highest classification and sensitivity level of the information involved.
13. Introduce wireless devices into FBI space without authorization from the ISSM.
14. Download, view, or send pornography or obscene material.
15. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.
16. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional.
17. 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.
18. Use internet “chat” services (e.g., AOL, Instant Messenger, Microsoft Network IM, Yahoo IM…etc).

19. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
20. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.
21. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).
22. Create or intentionally spread malicious code (i.e. viruses and Trojans).
23. Attempt to circumvent access controls/permissions or hack into (e.g., by penetration testing, password cracking, "sniffer" programs, etc.) any FBI IT/IS.
24. "Surf" through FBI files containing personal information merely for personal curiosity.
25. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.).
26. Use personal e-mail services (such as Yahoo, Gmail, etc.) for government business.
27. Download attachments via Outlook Web Access to a non-government computer.
28. Remove sensitive/classified media (paper or electronic) from controlled areas/facilities (i.e. taking classified media home) without authorization.

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 Exec. Order 9397, which permits 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. 12,968, Exec. Order No. 10,450, 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.

FD-889 Revised 12/05/08 Previous Versions Obsolete	FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form

The provision of the information is voluntary, but without your acknowledgment of the rules of behavior for accessing FBI information, and IT/IS's 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.

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

Fax: (304) 625-5399
1000 Custer Hollow Rd
Mod B-3
Clarksburg, WV 26306

Law Enforcement Online
Contractor Account 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**. When completed, fax or mail to the information provided in the upper right hand portion of page one of this form. **Send all pages, including the signed FD-889 Rules of Behavior form.** IMPORTANT: Non-legible applications will not be processed.

1. Contractor Applicant Information

Name (Last, First, MI):

Employing Company Name:

Title / Position:
(do not abbreviate)

E-mail Address:

Business Mailing Address:
(no PO Boxes)

Phone:

Alternate Phone:

2. Contractor Applicant Security Verification Information

Last 6 digits of Social Security Number:

XXX --

Date of Birth:

Code Word (ex: mother's maiden name):

3. FBI Sponsoring Party / Point of Contact

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:

4. Name and Description of Project, Justification of Access

Project Title:

Project Description:

Justification for Access:

Length of Access **From:** **To:**

Type of Access (Circle One): **LEO Email Only** **LEO Email & Specific SIG & VCC**

Specify Requested SIG & VCC Access Permissions:

5. Sponsoring Party / 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**

FD-889 Revised 12/05/08 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 does not apply to voice communications. This agreement form must be signed before access to any FBI IT/IS is granted.

References:

- Standards of Ethical Conduct Regulation (5 CFR Parts 2635 and 3801).
- The Federal Information Security Management Act (FISMA) of 2002.
- 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

Statement of Responsibility: I understand that I am to use FBI systems for lawful, official use and authorized purposes in accordance with current FBI guidelines. I am responsible for all IT that I introduce into FBI space including devices that are privately owned, or those owned by another government agency.

I am responsible for all activity on FBI IS's, as well as any other IT/IS's that are authorized to operate in FBI space, 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 activity when I am logged on an IS associated with that account.

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

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 I am prohibited from accessing or using information about individuals 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 individuals with sufficient care in order to ensure the security and confidentiality of the information and protect if from inadvertent or unauthorized disclosure. Even within the FBI and the Department of Justice, I am only permitted to disclose information about individuals on a need-to-know basis for performance of authorized tasks or mission related-functions. I am not permitted to disclose information about individuals outside the Department of Justice except when authorized under the Privacy Act (5 USC 552a(b)).

Access: Access to FBI IT, IS, networks, and other agency systems operating in FBI spaces is for official and authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations) (noted above) and as further outlined in this document.

Even where granted access, I must only access the system files and information on a need-to-know basis in furtherance of authorized tasks or mission related-functions.

Revocability: The ability to use IT in FBI space and access to FBI IS's is a revocable privilege. IT used in FBI space is subject to vulnerability assessment, content monitoring, activity monitoring, and security testing.

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's 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's accessed by me.
2. The following (2.a.) 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:
    a. 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.
4. I will comply with the FBI 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).
5. I will read and understand the FBI standard information system (IS) and network warning banner prior to logging onto the IS or network.

6. I will 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.
7. I will use FBI computer and network applications and systems, including but not limited to, e-mail, databases, and web services according to and in compliance with FBI policy directives.
8. I will ensure that I understand and respect the accredited security level of FBI facilities and of FBI IT systems that I work with or access.
9. I will protect my password(s) in accordance with the classification level of the system or at the highest classification of the data being secured.
10. I will only 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.
11. I will use screen locks or logoff my workstation upon departing the immediate area.
12. I will use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.
13. I will use only authorized media (thumb drives, diskettes, etc) and procedures to download FBI information.
14. I will 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 Coordination Office (CAPCO) guidelines, as appropriate.
15. I will 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.
16. When not in use, I will store classified computers in an approved security container, or in a facility approved for open storage of the information contained on that classified computer.
17. I will destroy copies and extracts of sensitive data that are no longer needed.
18. I will not disseminate any FBI non-public information to anyone who does not have a verified authorization to access the information and appropriate security clearance.
19. 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.
20. If designated as a "*Privileged User*" I will complete the required Privileged User Security training and sign the *Privileged User* Rules of Behavior form.
21. I will immediately report known or suspected security incidents or improper use to my ISSO, ISSM, or CSO according to SPM guidelines and FBI Policy Directives upon discovery regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information to the CSO according to the appropriate FBI incident response plan.
22. ***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 the "strong password" guidance mentioned in 4 and 5 above.

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.

23. 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.
24. 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.

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 authorize to operate in FBI space, unless required as part of my official duties:

1. Knowingly violate any statute or orders, such as compliance legislation, copyright laws or laws governing disclosure of information.
2. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).
3. 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.
4. Attempt to circumvent access controls or to use unauthorized means to gain access to accounts, files, folders or data on FBI IT/IS.
5. 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 from FBI IT without approval of my ISSO.
6. Permit any unauthorized individual access to a government-owned or government-operated system, device, or service.
7. Exhibit behaviors that could lead to damage, endangerment or degradation of FBI equipment, software, media, data, facilities, services, or people.
8. 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.
9. 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.
10. Connect classified IT or IS's to the Internet or other unclassified systems.
11. Attempt to process or enter information onto a system exceeding the authorized classification level. (e.g., placing Top Secret information on Secret Enclave).
12. Operate IT systems, whether fixed or portable, in areas or facilities that are not approved by the Assistant Director for Security for processing the highest classification and sensitivity level of the information involved.
13. Introduce wireless devices into FBI space without authorization from the ISSM.
14. Download, view, or send pornography or obscene material.
15. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.
16. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional.
17. 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.
18. Use internet “chat” services (e.g., AOL, Instant Messenger, Microsoft Network IM, Yahoo IM…etc).

19. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
20. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.
21. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).
22. Create or intentionally spread malicious code (i.e. viruses and Trojans).
23. Attempt to circumvent access controls/permissions or hack into (e.g., by penetration testing, password cracking, "sniffer" programs, etc.) any FBI IT/IS.
24. "Surf" through FBI files containing personal information merely for personal curiosity.
25. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.).
26. Use personal e-mail services (such as Yahoo, Gmail, etc.) for government business.
27. Download attachments via Outlook Web Access to a non-government computer.
28. Remove sensitive/classified media (paper or electronic) from controlled areas/facilities (i.e. taking classified media home) without authorization.

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 Exec. Order 9397, which permits 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. 12,968, Exec. Order No. 10,450, 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.

FD-889 Revised 12/05/08 Previous Versions Obsolete	FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form

The provision of the information is voluntary, but without your acknowledgment of the rules of behavior for accessing FBI information, and IT/IS's 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.

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

Fax: (304) 625-5399
1000 Custer Hollow Road
Module B-3
Clarksburg, WV 26306

Law Enforcement Online
LEO International 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 in the information requested. When completed, fax or mail to the information provided in the upper right hand portion of page one of this form. Send all pages. If you require additional space to include information, please attach extra sheets and reference the appropriate section. IMPORTANT: Non-legible applications will not be processed.

1. Applicant Information

Applicant Name (Surname/Family Name, First, MI) :	
Title / Position:	
Email Address:	
Employing Agency and/or Organization:	

Address: (no P.O. Boxes)	**Country of Birth:**
	Country of Residence:
Phone:	**Country of Citizenship:**
Fax:	**State/Providence/County:**
	City: Postal Code:

Are you a US Citizen? **Yes** **No** **Dual**

Please list all citizenships held other than US:

2. Security Verification Information

Passport #/Country &/or last 6 of SSN if US Citizen:	**Date of Birth:**
Code Word (ex: mother's maiden name):	**Gender:** **Male** **Female**

Are you a Law Enforcement Officer? **Yes** **No** **If other please specify:**

3. Applicant Certification

I hereby certify that I am an employee of the duly constituted law enforcement/criminal justice/public safety agency described above in this application and that I understand and consent to the terms of this application, including the provisions set out in the Warning and the Privacy Act Statement, and agree to abide by all such provisions.

X _____

APPLICANT SIGNATURE **MONTH / DAY / YEAR**

Instructions Sections 4,5,6: These areas are reserved for the LEGAT, ALAT, or Other FBI Designated Authority responsible for the requested account. Complete all requested information where applicable.

4. LEGAT / ALAT / Other FBI Designated Authority (Responsible Party)

Name (Last, First, MI):		
Legat/Division/Field Office:		
Title / Position:		
Email Address:		
Room Number:		
Address:	**Country:**	**Zip:**
	State / Prov:	**Phone:**
	City:	**Fax:**

5. Justification of Access, Name & Description of Project

Justification For Access:

Is this a Special Project? **Yes** **No**

Describe Special Project (if applicable):

Length of Access (if applicable) **From:** MONTH / DAY / YEAR **To:** MONTH / DAY / YEAR

Type of Access (Select One): **LEO Email Only** **LEO Email & Specific SIG** **Specify SIG:**

6. LEGAT / ALAT / Other FBI Designated Authority Certification (Please complete signature lines)

I hereby certify that the above named individual is an employee of the duly constituted agency and/or organization described above and is authorized to have access to the Law Enforcement Online (LEO) system.

X

SIGNATURE **MONTH / DAY / YEAR**

Please Print Name:

LEGAT / ALAT / Other FBI Designated Authority Administration

Instructions for LEGAT / ALAT / Other FBI Designated Authority Administration:	After completing and verifying this information submitted in this form, fax or mail entire application to FBI: **Fax: (304) 625-5399** LEO Program Office 1000 Custer Hollow Rd Module B-3 Clarksburg, WV 26306 Phone Number: (304) 625-5555

LEO Administration Only

Creation Date: MM/DD/YYYY **SIG** **VPN**

Authorized By:

X

LEO AUTHORIZATION SIGNATURE **SIGN AND PRINT NAME** **MONTH / DAY / YEAR**

Data Entry Verification

Completed By:

X

DATA ENTRY SIGNATURE **SIGN AND PRINT NAME** **MONTH / DAY / YEAR**

Comments

FD-889 Revised 12/05/08 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 does not apply to voice communications. This agreement form must be signed before access to any FBI IT/IS is granted.

References:

- Standards of Ethical Conduct Regulation (5 CFR Parts 2635 and 3801).
- The Federal Information Security Management Act (FISMA) of 2002.
- 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

Statement of Responsibility: I understand that I am to use FBI systems for lawful, official use and authorized purposes in accordance with current FBI guidelines. I am responsible for all IT that I introduce into FBI space including devices that are privately owned, or those owned by another government agency.

I am responsible for all activity on FBI IS's, as well as any other IT/IS's that are authorized to operate in FBI space, 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 activity when I am logged on an IS associated with that account.

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

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 I am prohibited from accessing or using information about individuals 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 individuals with sufficient care in order to ensure the security and confidentiality of the information and protect if from inadvertent or unauthorized disclosure. Even within the FBI and the Department of Justice, I am only permitted to disclose information about individuals on a need-to-know basis for performance of authorized tasks or mission related-functions. I am not permitted to disclose information about individuals outside the Department of Justice except when authorized under the Privacy Act (5 USC 552a(b)).

Access: Access to FBI IT, IS, networks, and other agency systems operating in FBI spaces is for official and authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations) (noted above) and as further outlined in this document.

Even where granted access, I must only access the system files and information on a need-to-know basis in furtherance of authorized tasks or mission related-functions.

Revocability: The ability to use IT in FBI space and access to FBI IS's is a revocable privilege. IT used in FBI space is subject to vulnerability assessment, content monitoring, activity monitoring, and security testing.

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's 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's accessed by me.
2. The following (2.a.) 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:
    a. 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.
4. I will comply with the FBI 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).
5. I will read and understand the FBI standard information system (IS) and network warning banner prior to logging onto the IS or network.

6. I will 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.
7. I will use FBI computer and network applications and systems, including but not limited to, e-mail, databases, and web services according to and in compliance with FBI policy directives.
8. I will ensure that I understand and respect the accredited security level of FBI facilities and of FBI IT systems that I work with or access.
9. I will protect my password(s) in accordance with the classification level of the system or at the highest classification of the data being secured.
10. I will only 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.
11. I will use screen locks or logoff my workstation upon departing the immediate area.
12. I will use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.
13. I will use only authorized media (thumb drives, diskettes, etc) and procedures to download FBI information.
14. I will 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 Coordination Office (CAPCO) guidelines, as appropriate.
15. I will 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.
16. When not in use, I will store classified computers in an approved security container, or in a facility approved for open storage of the information contained on that classified computer.
17. I will destroy copies and extracts of sensitive data that are no longer needed.
18. I will not disseminate any FBI non-public information to anyone who does not have a verified authorization to access the information and appropriate security clearance.
19. 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.
20. If designated as a "*Privileged User*" I will complete the required Privileged User Security training and sign the *Privileged User* Rules of Behavior form.
21. I will immediately report known or suspected security incidents or improper use to my ISSO, ISSM, or CSO according to SPM guidelines and FBI Policy Directives upon discovery regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information to the CSO according to the appropriate FBI incident response plan.
22. ***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 the "strong password" guidance mentioned in 4 and 5 above.

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.

23. 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.
24. 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.

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 authorize to operate in FBI space, unless required as part of my official duties:

1. Knowingly violate any statute or orders, such as compliance legislation, copyright laws or laws governing disclosure of information.
2. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).
3. 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.
4. Attempt to circumvent access controls or to use unauthorized means to gain access to accounts, files, folders or data on FBI IT/IS.
5. 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 from FBI IT without approval of my ISSO.
6. Permit any unauthorized individual access to a government-owned or government-operated system, device, or service.
7. Exhibit behaviors that could lead to damage, endangerment or degradation of FBI equipment, software, media, data, facilities, services, or people.
8. 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.
9. 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.
10. Connect classified IT or IS's to the Internet or other unclassified systems.
11. Attempt to process or enter information onto a system exceeding the authorized classification level. (e.g., placing Top Secret information on Secret Enclave).
12. Operate IT systems, whether fixed or portable, in areas or facilities that are not approved by the Assistant Director for Security for processing the highest classification and sensitivity level of the information involved.
13. Introduce wireless devices into FBI space without authorization from the ISSM.
14. Download, view, or send pornography or obscene material.
15. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.
16. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional.
17. 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.
18. Use internet “chat” services (e.g., AOL, Instant Messenger, Microsoft Network IM, Yahoo IM…etc).

19. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
20. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.
21. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).
22. Create or intentionally spread malicious code (i.e. viruses and Trojans).
23. Attempt to circumvent access controls/permissions or hack into (e.g., by penetration testing, password cracking, "sniffer" programs, etc.) any FBI IT/IS.
24. "Surf" through FBI files containing personal information merely for personal curiosity.
25. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.).
26. Use personal e-mail services (such as Yahoo, Gmail, etc.) for government business.
27. Download attachments via Outlook Web Access to a non-government computer.
28. Remove sensitive/classified media (paper or electronic) from controlled areas/facilities (i.e. taking classified media home) without authorization.

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 Exec. Order 9397, which permits 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. 12,968, Exec. Order No. 10,450, 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.

FD-889 Revised 12/05/08 Previous Versions Obsolete	FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form

The provision of the information is voluntary, but without your acknowledgment of the rules of behavior for accessing FBI information, and IT/IS's 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.

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

LAW ENFORCEMENT ONLINE

Please select the appropriate form:

- N-DEx/OneDoJ User Application Form
- N-DEx/OneDoJ Bulk Verification
- N-DEx/OneDoJ Cancellation of Access

LEO Support Center

(888) 334-4LEO (4536)
TTY: (304) 625-3963

N-DEx / OneDOJ User Application

Fax Completed Application To: (888) 550-6427

WARNING ▶▶▶ LEO / N-DEx / OneDOJ are official U.S. Government systems for authorized use only by authorized members of the law enforcement, criminal justice and public safety community. Information presented in these systems is considered sensitive but unclassified and is for official law enforcement/criminal justice/public safety use only. The use of these services & systems will be monitored for security and administration purposes and accessing these services & systems constitutes consent to such monitoring. Any unauthorized access of them or unauthorized use of the information provided by these systems is prohibited and may be subject to criminal and civil penalties under federal law, state, and other.

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

Warning! The use of publicly accessible computers (e.g. libraries, airports, cafes, hotels, etc.) to access these systems are 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 the LEO / N-DEx / OneDOJ User Application forms. Authority - LEO / N-DEx / OneDOJ are federally funded national systems 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 purpose of the LEO / N-DEx / OneDOJ 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 / N-DEx and/or OneDOJ account. All or part of the submitted information may be disclosed outside the FBI to federal, state, local, county, 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 these systems. 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.

WARNING! The N-DEx and OneDOJ systems are restricted law enforcement databases that are the property of, and maintained by, the United States Department of Justice (DOJ), Federal Bureau of Investigation (FBI). Access to these systems is restricted to authorized government personnel for official purposes. These systems will be audited and monitored for improper use by an individual and/or organization. Anyone accessing and using these databases expressly consents to such monitoring and recording for law enforcement and other purposes. Misuse of the systems by any individual and/or organization by any non-authorized user or for other than its intended purposes are prohibited and will result in the termination of use and other sanctions which may include administrative or criminal prosecution.

These systems are for authorized law enforcement purposes, including but not limited to, criminal investigations, homeland security, and national security. All N-DEx system users consent to follow established policies as defined in the *Law Enforcement N-DEx Policy Manual*.

Each contributor retains sole ownership of and sole responsibility for the information submitted to the N-DEx System. Therefore, each contributor will have an obligation to maintain system discipline which includes the timeliness, completeness, and accuracy of the data they contribute to the system. Prior to taking any law enforcement action using information from the N-DEx, concurrence from the contributing agency (owner of the record) must be obtained. That is, the information from the N-DEx cannot be incorporated into the using agency's case file, used for any official action (e.g. affidavit for search and/or arrest), or further disseminated without such concurrence.

Immediate dissemination of the N-DEx information can be made without the permission of the contributing agency if: (a) there is an actual or potential threat of terrorism, immediate danger of death or serious physical injury to any person, or imminent harm to public safety or national security; and (b) it is necessary to disseminate such information without delay to any appropriate recipient for the purpose of preventing or responding to that threat. The contributing agency (owner of the record) shall be immediately notified of any dissemination made under this exception.

Information in the N-DEx and OneDOJ may only be secondarily disseminated to law enforcement or authorized law enforcement representatives, as defined above, pursuant to a Memorandum of Understanding or User Agreement and consistent with the uses identified within the FBI's Privacy Act Systems of Records Notice published in the Federal Register. Neither the U.S. DOJ nor the FBI is responsible for the accuracy of contributing party's information or misuse of the Systems.

9999808001

INSTRUCTIONS:

1. User Application and FD-889 Rules of Behavior User Agreement: Applicant must complete the application in its entirety to include the approving agency level signature in block #4 and CJIS Systems Officer / N-DEx Point of Contact (CSO / POC) signature in block #5. For the N-DEx system, local law enforcement agencies should route requests through their CSO / POC for approving signature.

Type or write in the information requested. You may use Adobe Acrobat to fill, save and print this form. Use the mouse to insert the cursor in a field or click check boxes. Upon completion, to include appropriate signatures, fax the information to (888) 550-6427. IMPORTANT: Non-legible applications will not be processed.

ADDITIONAL FORM (optional): Bulk Verification Request - This form may be used at the agency level and/or the CSO / POC level as it allows approval of multiple access requests with one signature and can be signed rather than Section 4 and/or 5 of each User Application. You can submit one signed *Bulk Verification* form with a list of names which correspond with the **accompanying User Applications**, rather than sign each application separately.

A LEO account is required for access to the N-DEx System and is optional for the OneDOJ System.

Choose the applicable LEO selection:

☐ **Existing LEO UserID:** _____ **ORI:** _____

☐ **New LEO User** **ORI:** _____

Must be a valid 9 digit ORI (Originating Agency Identifier) and will be used to provide NCIC / III returns to eligible users.

I request access to:

☐ **N-DEx**

FOR ATF, BOP, DEA, EOUSA, FBI, USMS or DOJ AUTHORIZED USERS ONLY:

☐ **OneDOJ** – LEO access to the OneDOJ ☐ **OneDOJ** – Direct access to OneDOJ

1. Applicant Information	
Name (Last, First, MI) :	Postfix:
Title / Position:	
Email Address:	
Are you a US citizen? ☐ Yes ☐ No ☐ Dual	Please list all citizenships held other than US:
Are you an Intelligence Analyst? ☐ Yes ☐ No	Are you a RISS User? ☐ Yes ☐ No
APPLICANT SECURITY VERIFICATION INFORMATION	
Date of Birth: __ __/__ __/__ __ __ __	
SSN - last six digits: XXX - __ __ - __ __ __ __	Code Word (ex: Mother's Maiden Name):
Are you a Sworn Law Enforcement Officer (arresting powers)? ☐ Yes ☐ No	

2. EMPLOYING AGENCY / ORGANIZATION INFORMATION (ELIGIBILITY: U.S., U.S. Territories, U.S. Possessions Only)	
Agency / Org Name:	
Agency / Org Jurisdiction: ☐ Federal ☐ State ☐ Local ☐ County ☐ Tribal	
Agency / Org Type: ☐ Law Enforcement ☐ Military ☐ First Responders ☐ Government/Other	Specify Government/Other:
Physical Address:	City:
	State / Prov: County:
Phone:	Zip:
Fax:	Country:

9999808001

ALTERNATE MAILING ADDRESS (If needed)

Address:	City:
	State / Prov: County:
Phone:	Zip:
Fax:	Country:

3. APPLICANT CERTIFICATION

I hereby certify that I am an employee of the duly constituted Law Enforcement / Criminal Justice / Public Safety Agency described above in this application and that I understand and consent to the terms of this application, including the provisions set out in the above Warning and the Privacy Act Statement listed above, and agree to abide by all such provisions.

Applicant Signature: _____ **Date:** __/__/____

4. AGENCY HEAD (OR DESIGNEE) APPROVAL OF APPLICANT REQUIRED (Please complete signature lines)

I hereby certify that the above named individual is an employee of the duly constituted agency described above and is authorized access to the requested services and system(s).

Agency Level Signature: _____ **Date:** __/__/____

Please Print Name: _____ **Title:** _____

5. CSO / POC (OR DESIGNEE) APPROVAL OF APPLICANT REQUIRED (Please complete signature lines)

I hereby certify that the above named individual is an employee of the duly constituted agency described above and is authorized access to the requested services and system(s).

Do you approve this applicant to have NCIC and/or III user privileges via N-DEx? If so, check the appropriate box(es):

☐ NCIC* ☐ III* * **Must Provide Most Recent NCIC Certification / Re-certification Date:** __/__/____

CSO / POC Level Signature: _____ **Date:** __/__/____

Please Print Name: _____ **Title:** _____

Fax Completed Applications To The N-DEx/OneDOJ Authentication Office at 1-888-550-6427

N-DEx / OneDOJ ADMINISTRATION ONLY

Creation Date: __/__/____ SIG VPN

Authorized by: _____

N-DEx / OneDOJ AUTHORIZATION SIGNATURE PRINT NAME MONTH / DAY / YEAR

LEO ADMINISTRATION ONLY

Creation Date: __/__/____ SIG VPN

Authorized by: _____

LEO AUTHORIZATION SIGNATURE PRINT NAME MONTH / DAY / YEAR

DATA ENTRY VERIFICATION

Completed by: _____

DATA ENTRY SIGNATURE PRINT NAME MONTH / DAY / YEAR

N-DEx/OneDOJ Authentication Office, Module B-3
Federal Bureau of Investigation
Criminal Justice Information Services Division
1000 Custer Hollow Road, Clarksburg, WV 26306

FD-889 Revised 12/05/08 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 does not apply to voice communications. This agreement form must be signed before access to any FBI IT/IS is granted.

References:

- Standards of Ethical Conduct Regulation (5 CFR Parts 2635 and 3801).
- The Federal Information Security Management Act (FISMA) of 2002.
- 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

Statement of Responsibility: I understand that I am to use FBI systems for lawful, official use and authorized purposes in accordance with current FBI guidelines. I am responsible for all IT that I introduce into FBI space including devices that are privately owned, or those owned by another government agency.

I am responsible for all activity on FBI IS's, as well as any other IT/IS's that are authorized to operate in FBI space, 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 activity when I am logged on an IS associated with that account.

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

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 I am prohibited from accessing or using information about individuals 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 individuals with sufficient care in order to ensure the security and confidentiality of the information and protect if from inadvertent or unauthorized disclosure. Even within the FBI and the Department of Justice, I am only permitted to disclose information about individuals on a need-to-know basis for performance of authorized tasks or mission related-functions. I am not permitted to disclose information about individuals outside the Department of Justice except when authorized under the Privacy Act (5 USC 552a(b)).

Access: Access to FBI IT, IS, networks, and other agency systems operating in FBI spaces is for official and authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations) (noted above) and as further outlined in this document.

Even where granted access, I must only access the system files and information on a need-to-know basis in furtherance of authorized tasks or mission related-functions.

Revocability: The ability to use IT in FBI space and access to FBI IS's is a revocable privilege. IT used in FBI space is subject to vulnerability assessment, content monitoring, activity monitoring, and security testing.

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's 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's accessed by me.
2. The following (2.a.) 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:
    a. 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.
4. I will comply with the FBI 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).
5. I will read and understand the FBI standard information system (IS) and network warning banner prior to logging onto the IS or network.

6. I will 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.
7. I will use FBI computer and network applications and systems, including but not limited to, e-mail, databases, and web services according to and in compliance with FBI policy directives.
8. I will ensure that I understand and respect the accredited security level of FBI facilities and of FBI IT systems that I work with or access.
9. I will protect my password(s) in accordance with the classification level of the system or at the highest classification of the data being secured.
10. I will only 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.
11. I will use screen locks or logoff my workstation upon departing the immediate area.
12. I will use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.
13. I will use only authorized media (thumb drives, diskettes, etc) and procedures to download FBI information.
14. I will 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 Coordination Office (CAPCO) guidelines, as appropriate.
15. I will 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.
16. When not in use, I will store classified computers in an approved security container, or in a facility approved for open storage of the information contained on that classified computer.
17. I will destroy copies and extracts of sensitive data that are no longer needed.
18. I will not disseminate any FBI non-public information to anyone who does not have a verified authorization to access the information and appropriate security clearance.
19. 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.
20. If designated as a "*Privileged User*" I will complete the required Privileged User Security training and sign the *Privileged User* Rules of Behavior form.
21. I will immediately report known or suspected security incidents or improper use to my ISSO, ISSM, or CSO according to SPM guidelines and FBI Policy Directives upon discovery regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information to the CSO according to the appropriate FBI incident response plan.
22. ***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 the "strong password" guidance mentioned in 4 and 5 above.

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.

23. 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.
24. 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.

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 authorize to operate in FBI space, unless required as part of my official duties:

1. Knowingly violate any statute or orders, such as compliance legislation, copyright laws or laws governing disclosure of information.
2. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).
3. 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.
4. Attempt to circumvent access controls or to use unauthorized means to gain access to accounts, files, folders or data on FBI IT/IS.
5. 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 from FBI IT without approval of my ISSO.
6. Permit any unauthorized individual access to a government-owned or government-operated system, device, or service.
7. Exhibit behaviors that could lead to damage, endangerment or degradation of FBI equipment, software, media, data, facilities, services, or people.
8. 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.
9. 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.
10. Connect classified IT or IS's to the Internet or other unclassified systems.
11. Attempt to process or enter information onto a system exceeding the authorized classification level. (e.g., placing Top Secret information on Secret Enclave).
12. Operate IT systems, whether fixed or portable, in areas or facilities that are not approved by the Assistant Director for Security for processing the highest classification and sensitivity level of the information involved.
13. Introduce wireless devices into FBI space without authorization from the ISSM.
14. Download, view, or send pornography or obscene material.
15. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.
16. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional.
17. 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.
18. Use internet "chat" services (e.g., AOL, Instant Messenger, Microsoft Network IM, Yahoo IM...etc).

19. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
20. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.
21. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).
22. Create or intentionally spread malicious code (i.e. viruses and Trojans).
23. Attempt to circumvent access controls/permissions or hack into (e.g., by penetration testing, password cracking, "sniffer" programs, etc.) any FBI IT/IS.
24. "Surf" through FBI files containing personal information merely for personal curiosity.
25. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.).
26. Use personal e-mail services (such as Yahoo, Gmail, etc.) for government business.
27. Download attachments via Outlook Web Access to a non-government computer.
28. Remove sensitive/classified media (paper or electronic) from controlled areas/facilities (i.e. taking classified media home) without authorization.

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 Exec. Order 9397, which permits 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. 12,968, Exec. Order No. 10,450, 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.

FD-889 Revised 12/05/08 Previous Versions Obsolete	FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form

The provision of the information is voluntary, but without your acknowledgment of the rules of behavior for accessing FBI information, and IT/IS's 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.

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

N-DEx / OneDOJ User Application Bulk Verification Form

Fax Completed Applications To: (888) 550-6427

The *Bulk Verification Form* is used at the CSO/POC and/or local agency level when it will be cumbersome to sign mass quantities of N-DEx/ OneDOJ User Applications. This listing should mirror those individuals whose User Applications are being submitted.

***If Bulk Verification form is used at agency level, it must be routed for state level (CSO) approval as well.**

1. Agency Head (or Designee) Approving Signature (All User Applications Must Have Agency Level and State Level Approval)

I hereby certify the individuals listed below are employees of the duly constituted agency described in the attached documents and are authorized access to the requested services and system(s).

Signature: _____ Date: __/__/____

Please Print Name: _____ Title: _____

2. CSO / POC (or Designee) Approving Signature

I hereby certify the individuals listed below are employees of the duly constituted agency described in the attached documents and are authorized access to the requested services and system(s).

Signature: _____ Date: __/__/____

Please Print Name: _____ Title: _____

Please provide FULL NAME, AGENCY NAME, and ORI of the individual(s) this verification form is to cover. Also indicate if individual is approved to access NCIC and/or III via N-DEx and provide the most recent Certification / Recertification Date, if applicable.

NAME	AGENCY	ORI #	Approval to access NCIC and/or III via N-DEx? Check appropriate box(es)
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____
			☐ NCIC ☐ III – Current NCIC Certification/Recertification Date __/__/____

9999808002

N-DEx / OneDOJ
Cancellation of Access Form

Fax To: (888) 550-6427

The *Cancellation of Access* form notifies the N-DEx / OneDOJ Authentication Office of those individuals requiring termination of their Services & System(s) access. Please provide the full name, agency name, and ORI of the individual(s) to be cancelled. Include additional sheets as necessary. This form may be used at both the Agency and State Level.

1. Agency Head Signature

I hereby certify the listed individual requires termination of access to the services & system(s) as described below.

Signature: _____ Date: __/__/_____

Please Print Name: _____ Title: _____

2. CSO / POC (or Designee) Signature

I hereby certify the listed individual requires termination of access to the services & system(s) as described below.

Signature: _____ Date: __/__/_____

Please Print Name: _____ Title: _____

PLEASE LIST FULL NAME, AGENCY NAME, ORI and SYSTEM of the individual(s) requiring access termination.

NAME	AGENCY	ORI #	SYSTEM
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ
			☐ N-DEx ☐ OneDOJ

9999808002