FD-889 Revised 04-01-2019 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 any FBI Information Technology (IT) and Information System (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.) and not to voice communications. This agreement form must be signed before access to any FBI IT/IS is granted.

Monitoring and Search Notification/Consent: I consent to the search of any IT/IS equipment or media I bring into, or remove from FBI owned, controlled or leased facilities as authorized by law. When asked by authorized personnel, I will provide access to all equipment or media brought into or removed from such FBI controlled facilities upon reasonable suspicion of unauthorized activities.

I also understand that FBI or FBI leased IS may be monitored or otherwise accessed for law enforcement, security, counterintelligence or other compliance purposes and my agreement to these FBI Rules of Behavior (ROB) constitutes my consent to be monitored, to allow access to all FBI IS accessed by me, and to permit an aggregated review of all of my system/network activities and data base entries and activities.

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

> I understand that the aforementioned IT/IS assets are also subject to FBI search; however, prior to any search, 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.

Statement of Responsibility: I understand that I am to use FBI systems only for lawfully authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations), 28 CFR 45.4 (de minimis personal use), and as further outlined in this document and other FBI policy directives. Even where granted access, I must access the system files and information only on a need-to-know basis and only in furtherance of authorized tasks or mission related-functions. To remain compliant with applicable statutes, orders, regulations, and directives, the FBI will update this form. It is my responsibility to maintain current knowledge of the FBI IT/IS Rules of Behavior for General Users.

I am responsible for all activity on any FBI IS occurring on my individual account(s) once my logon credential or password has been used to logon. If I am a member of a "group

account," I am responsible for all of my activity when I am logged on an IS associated with that account.

As an authorized user of FBI IT/IS, I acknowledge the responsibility to protect FBI information. I also acknowledge the responsibility to protect FBI information when using OGA IT/IS assets in FBI controlled facilities.

I am responsible for all IT that I introduce into FBI controlled facilities.

I acknowledge that it is my responsibility to ensure the proper marking, storage, protection, and disposition of all non-public information to which I am given access as a result of my work with the FBI.

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

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

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

1. I will read and adhere to all FBI information assurance policy directives, including the *Polygraph Program Policy Guide* (0798PG), FBI Policy Directives, and local Standard Operating Procedures (SOP). I will use FBI IT/IS, including, but not limited to email, databases, and web services, according to and in compliance with FBI policies.

2. 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).

3. I will complete the FBI's Annual Information Security (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.

4. I will immediately report known or suspected security incidents or improper use of FBI IT/IS to my CSO according to Security Compliance Program Policy Guide (0934PG) and the Roles and Responsibilities for Reporting a Data Breach Policy Directive (0504D) upon discovery, regardless of whether such action results in loss of control or unauthorized disclosure of sensitive information.

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

    a. Ensure I understand and respect the authorized security level of FBI controlled facilities and of FBI IT/IS and IT/IS owned or managed by OGA I work with or access pursuant to my FBI duties.

b. Use only authorized Video Teleconferencing (VTC) sessions and ensure persons who are not involved in the session cannot see or hear the content of the session.

b7E

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

a. Operate FBI IT systems and technology processing classified information only in a facility that is approved for the highest classification level of the information contained on the IT system or technology. When not in use, I will store classified computers and electronic storage media in an approved security container or in a facility approved for open storage of the information that the device or system contains.
b. Operate FBI IT systems processing sensitive unclassified (e.g. For Official Use Only, Law Enforcement Sensitive) information only in a facility approved for processing of sensitive unclassified information. When not in use, I will store sensitive unclassified computers and electronic storage media in a facility approved for storage of the information that the device or system contains.
c. Read the FBI warning banner that is presented prior to IS or network log on.
d. Use FBI peripheral devices (embedded and add-on) according to and in compliance with FBI policies. Examples of peripheral devices are cameras, microphones, storage devices, and telephones.
e. Use FBI IT equipment, including but not limited to PEDs, keyboard, video, monitor (KVM) switch devices, and wireless technologies according to and in compliance with FBI policies.
f. Use only properly licensed FBI-approved software and hardware.
g. Protect all copyright and other intellectual property rights according to terms and conditions contained in FBI approved software and hardware licenses.
h. Use strong passwords as defined by FBI policies and procedures, and agree to change my password with a frequency as specified by policy or as requested for security reasons.
i. Use unique passwords for each account.
j. Protect my password(s) according to the classification level of the system or at the highest classification of the data being secured. I will protect my passwords from disclosure to other people.
k. Use screen locks or logoff my workstation upon departing my immediate work area for any length of time.
l. Log off all IS at the end of each day.
m. Use only authorized electronic storage media (USB memory, CDs, DVDs, zip drives, floppy diskettes) and procedures to download or store FBI information.
n. Use government provided virus-checking procedures before accessing information from all removable storage media or before accessing email attachments.
o. Properly mark and label classified and sensitive information and media (removable and fixed) according to FBI policy.
p. Encrypt, using FBI-approved solutions, all sensitive and classified data stored on portable electronic or optical media, and data stored on computers that are transported outside of FBI controlled facilities.
q. Use FBI-approved Cross Domain Data Transfer procedures for every transfer of information between FBI security domains.

r. Verify that each computer-readable data extract including sensitive data has been erased within 90 days of origination or its use is still required.
s. Disseminate any FBI non-public information only to persons who have a verified authorization to access the information and appropriate security clearance.

7. While traveling on FBI business with FBI IT/IS, I will:
   a. Limit information on my accessible FBI IT systems and components to what is needed to perform my FBI mission.
   b. Power down IT/IS when possible and not needed.
   c. Disable wireless capabilities of any wireless-capable device when the capability is not in use.
   d. Not use Internet Cafes or other public WiFi® locations to conduct official business.
   e. Prior to traveling overseas or to a foreign nation, attend all required overseas travel briefings.

8. If approved to Telework, I will comply with the policies and procedures identified in the Telework Policy (0406D).

9. ***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 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 controlled facilities, or in my home.
   d. Use strong passwords.
   e. Immediately request my ISSO, ISSM, or CSO or an authorized FBI PKI authority to revoke my associated credentials if I suspect that my token or keys are lost/stolen or if my password was compromised.

Expressly Prohibited Behavior: Unless required as part of official duties, the following behaviors or activities are prohibited on any FBI IT/IS authorized to operate by the FBI or on other agency IT/IS authorized to operate in FBI controlled facilities.

I will not:

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

   a. Attempt to process or enter information onto a system exceeding the authorized classification level for that IT/IS (e.g., placing Secret information on an Unclassified IT/IS).
   b. Connect classified IT/IS to the Internet or other unclassified systems.
   c. Remove sensitive/classified media (paper or electronic) from controlled areas/facilities (i.e. taking classified media home) without authorization.

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

2. Misuse my FBI IT/IS privileges including:

a. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).
b. Permit any unauthorized person access to a government-owned or government-operated system, device, or service.
c. Use an account, user ID, or password not specifically assigned to me, masquerade as another user, or otherwise misrepresent my identity and privileges to IT/IS administrators and security personnel.

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

a. Attempt to circumvent access controls or to use unauthorized means (e.g., penetration testing, password cracking, "sniffer" programs), to gain access to accounts, files, folders or data on FBI IT/IS.
b. Change configuration settings of operating systems or security related software, or remove, modify, or add any hardware or software to/from FBI IT/IS without approval of my ISSO.
c. Alter, change, configure, install software or hardware, or connect IT or systems or otherwise tamper with my computer to circumvent any FBI policy and IT/IS protections.
d. Open e-mails or other messages from suspicious sources (e.g., sources that you do not recognize as legitimate for your line of business).
e. Create or intentionally spread malicious code (i.e. viruses and Trojans).
f. Attempt to access any security audit trail information that may exist without authorization.
g. Download software or executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) from any non-FBI sites, including social networking sites, without authorization.
h. Install or connect non-FBI owned or leased (including privately owned) software or hardware and removable electronic storage (RES) to FBI IT/IS without authorization.
i. Use the facilities of Internet cafés or other public Wi-Fi® locations to conduct official business.

4. On FBI IT, except as authorized for investigatory purposes, participate in prohibited activities, including but not limited to:

a. Download, view, or send pornography or obscene material.
b. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.
c. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional according to FBI standards of professional behavior.
d. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.
e. Use internet "chat" services (e.g., AOL, Instant Messenger (IM), Microsoft Network IM, Yahoo IM…etc).
f. Use publicly available social networking sites for personal use.

g. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
h. "Surf" through FBI files containing personal information for unofficial purposes.
i. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.).
j. Use personal e-mail services (such as Yahoo, Gmail, etc.) for government business.
k. Download attachments via Outlook Web Access to a non-government computer.

Privacy Act Statement:

The information solicited on this form is collected pursuant to the Federal Information Security Management Act (FISMA) of 2002, the Computer Security Act of 1987, the general recordkeeping provision of the Administrative Procedures Act (5 U.S.C. § 301) and Executive Order 9397, as amended by Executive Order 13478, which permits the collection of social security numbers.

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

The principal purpose of this form is to verify that individual signatories are aware of the rules of behavior that govern access to FBI IT/IS operating in FBI controlled facilities. 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 with Department of Justice (DOJ) components and with other governmental agencies for the purpose of facilitating information sharing (i.e., sending encrypted e-mails) and for other authorized purposes.

In addition, information may be disclosed to the following;

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

The provision of the information is voluntary, but without your acknowledgment of the rules of behavior for accessing FBI information, and IT/IS that operate in FBI controlled facilities, 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 that could result 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): _____

If applicable, other Govt. Agency (Federal, state, or municipality) _____

Filing Instructions: Completion of the FBI's annual INFOSEC Awareness Training satisfies 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.

References:

- Standards of Ethical Conduct Regulation (5 CFR Parts 2635 and 3801).
- US Code, Title 18, Section 798.
- The Privacy Act of 1974 (as amended) 5 USC 552a.
- The Federal Information Security Management Act (FISMA) of 2002.
- Executive Order 10450, Security Requirements for Government Employment.
- Executive Order 12968, Access to Classified Information.
- Executive Order 13478, Federal Agency Use of Social Security Numbers.
- National Security Telecommunications and Information Systems Security Advisory Memoradum (NSTISSAM) 2-95 Red/Black Installation Guidance.
- NSTISSAM 2-95-A amendment to 2-95.
- Office of Management and Budget (OMB) Circular A-130.
- Department of Justice (DOJ) Order 2640.2F, Information Technology Security.
- DOJ Order 2740.1a, Use and Monitoring of DOJ Computers and Computer Systems
- DOJ IT Security Standard.
- Internal Revenue Service Code, sections 7213 and 7213 A (USC 26, 7213).
- Policy Directive 0061D, Consent to Warrantless Search Filing Requirement.
- Policy Directive 0922D, Information System Use.
- Security Monitoring of FBI Information Systems Policy Guide, 0655PG-3.
- Policy Directive 0146D, Personally Owned Storage Media.
- Security Compliance Program Policy Guide, 0934PG.
- Policy Directive 0636D, External Security Marking of Information Technology Hardware and Electronic Data Storage
- Policy Directive 0247D, Removable Electronic Storage (RES) Media Protection.
- Policy Directive 0627D, Video and Audio Teleconferencing (VTC).
- Mobile Devices and Mobile Applications Policy Guide, 0879PG.
- Cross Domain Management Policy Guide, 0655PG-5.
- Policy Directive 0633D, Keyboard, Video Monitor, and Mouse (KVM) Switches.
- Policy Directive 0299D, Privacy Policy Guide.
- Policy Directive 0335D, Image Capturing Devices within FBI Controlled Facilities.
- Security Assessment and Authorization Policy Guide, 0655PG.
- Telework Policy Guide, 1017PG.
- Policy Directive 0504D, Roles and Responsibilities for Reporting a Data Breach.
- Policy Directive 0723D, FBI Unclassified Network (UNet) Enclave Policy.
- U.S. Department of Justice (DOJ) Public Key Infrastructure X.509 Certificate Policy v1.13, December 15, 2006.
- X.509 Certification Practices Statement for the Federal Bureau of Investigation High Assurance Certificate Authority v3.2, January 22, 2009.
- 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.
- FD-1001 DOJ Consent For Warrantless Searches Of Department Of Justice Workplaces.
- SF-312, Classified Information Nondisclosure Agreement.
- Form 4414, Sensitive Compartmented Information Nondisclosure Agreement.
- Polygraph Progam Policy Guide, 0798PG.