



May 14, 2021

MR. JOHN GREENEWALD JR.  
SUITE 1203  
27305 WEST LIVE OAK ROAD  
CASTAIC, CA 91384-4520

FOIPA Request No.: 1389336-000  
Subject: FBI Directives and/or Memos Regarding  
Installing Unlicensed/Pirated Software on  
Government Computers

Dear Mr. Greenewald:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemption boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

<b>Section 552</b>		<b>Section 552a</b>
<input type="checkbox"/> (b)(1)	<input type="checkbox"/> (b)(7)(A)	<input type="checkbox"/> (d)(5)
<input type="checkbox"/> (b)(2)	<input type="checkbox"/> (b)(7)(B)	<input type="checkbox"/> (j)(2)
<input checked="" type="checkbox"/> (b)(3)	<input checked="" type="checkbox"/> (b)(7)(C)	<input type="checkbox"/> (k)(1)
<u>50 USC, Section 3024 (l)(1)</u>	<input type="checkbox"/> (b)(7)(D)	<input type="checkbox"/> (k)(2)
_____	<input checked="" type="checkbox"/> (b)(7)(E)	<input type="checkbox"/> (k)(3)
_____	<input type="checkbox"/> (b)(7)(F)	<input type="checkbox"/> (k)(4)
<input type="checkbox"/> (b)(4)	<input type="checkbox"/> (b)(8)	<input type="checkbox"/> (k)(5)
<input type="checkbox"/> (b)(5)	<input type="checkbox"/> (b)(9)	<input type="checkbox"/> (k)(6)
<input checked="" type="checkbox"/> (b)(6)		<input type="checkbox"/> (k)(7)

97 page(s) were reviewed and 97 page(s) are being released.

Please see the paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

- Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].
- This information has been referred to the OGA(s) for review and direct response to you.
- We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. "Part 1" of the Addendum includes standard responses that apply to all requests. "Part 2" includes additional standard responses that apply to all requests for records about yourself or any third party individuals.

“Part 3” includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

For questions regarding our determinations, visit the [www.fbi.gov/foia](http://www.fbi.gov/foia) website under “Contact Us.” The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

If you are not satisfied with the Federal Bureau of Investigation’s determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP’s FOIA STAR portal by creating an account following the instructions on OIP’s website: <https://www.justice.gov/oip/submit-and-track-request-or-appeal>. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked “Freedom of Information Act Appeal.” Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at [ogis@nara.gov](mailto:ogis@nara.gov); telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769. Alternatively, you may contact the FBI’s FOIA Public Liaison by emailing [foipaquestions@fbi.gov](mailto:foipaquestions@fbi.gov). If you submit your dispute resolution correspondence by email, the subject heading should clearly state “Dispute Resolution Services.” Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

See additional information which follows.

Please be advised that the Record/Information Dissemination Section (RIDS) is operating at reduced staffing levels amidst the ongoing COVID-19 national emergency. The enclosed FOIPA release represents a work product that could be generated for you under these unprecedented circumstances. We appreciate your patience and understanding as we work to release as much information, to as many requesters as possible, as this emergency continues.

The enclosed documents represent the final release of information responsive to your Freedom of Information/Privacy Acts (FOIPA) request.

Sincerely,



Michael G. Seidel  
Section Chief  
Record/Information  
Dissemination Section  
Information Management Division

Enclosure(s)

## FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.

### Part 1: The standard responses below apply to all requests:

- (i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on the [www.fbi.gov/foia](http://www.fbi.gov/foia) website.
- (ii) **Intelligence Records.** To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that any such records do or do not exist.

### Part 2: The standard responses below apply to all requests for records on individuals:

- (i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.
- (ii) **Requests for Records about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.
- (iii) **Requests for Records for Incarcerated Individuals.** The FBI can neither confirm nor deny the existence of records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA exemptions (b)(7)(E), (b)(7)(F), and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (b)(7)(F), and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

### Part 3: General Information:

- (i) **Record Searches.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems or locations where responsive records would reasonably be found. A standard search normally consists of a search for main files in the Central Records System (CRS), an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. Unless specifically requested, a standard search does not include references, administrative records of previous FOIPA requests, or civil litigation files. For additional information about our record searches, visit [www.fbi.gov/services/information-management/foipa/requesting-fbi-records](http://www.fbi.gov/services/information-management/foipa/requesting-fbi-records).
- (ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.
- (iii) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheet. These criminal history records are not the same as material in an investigative “FBI file.” An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at [www.fbi.gov/about-us/cjis/identity-history-summary-checks](http://www.fbi.gov/about-us/cjis/identity-history-summary-checks). Additionally, requests can be submitted electronically at [www.edo.cjis.gov](http://www.edo.cjis.gov). For additional information, please contact CJIS directly at (304) 625-5590.
- (iv) **National Name Check Program (NNCP).** The mission of NNCP is to analyze and report information in response to name check requests received from federal agencies, for the purpose of protecting the United States from foreign and domestic threats to national security. Please be advised that this is a service provided to other federal agencies. Private Citizens cannot request a name check.

## EXPLANATION OF EXEMPTIONS

### SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552


- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information ( A ) could reasonably be expected to interfere with enforcement proceedings, ( B ) would deprive a person of a right to a fair trial or an impartial adjudication, ( C ) could reasonably be expected to constitute an unwarranted invasion of personal privacy, ( D ) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, ( E ) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or ( F ) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

### SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

This document is made available through the declassification efforts  
and research of John Greenewald, Jr., creator of:

# The Black Vault



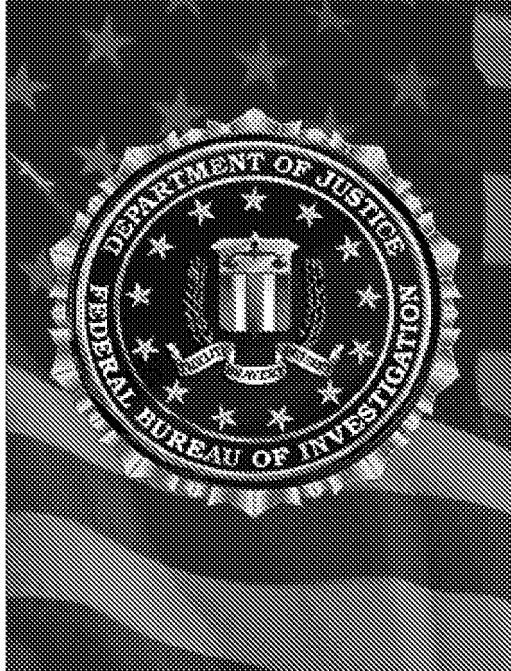
The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

**Discover the Truth** at: <http://www.theblackvault.com>

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

## **Mobile Devices and Mobile Applications Policy Guide**



**Federal Bureau of Investigation**

**Security Division and  
Information Technology Infrastructure Division**

**0879PG**

**July 6, 2016**

Revised: 10/30/2017

**UNCLASSIFIED**

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

**General Information**

Questions or comments pertaining to this policy guide can be directed to:

Federal Bureau of Investigation Headquarters

Security Division (SecD) or Information Technology Infrastructure Division (ITID) point of contact: SecD division policy officer (DPO) or Mobility Program Office (MPO) supervisor

**Supersession Information**

This document supersedes Policy Directive 0256D, *Portable Electronic Devices (PEDs)*.

This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit listed in the contact section of this policy guide.

This document is intended solely for providing internal FBI guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor does it place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice and the FBI.

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

**Table of Contents**

**1. Introduction**..... 1

1.1. Purpose..... 1

1.2. Background ..... 1

1.2.1. Accountability and Waste Prevention..... 1

1.2.2. Intelligence and Law Enforcement Community Engagement and Leadership..... 1

1.2.3. Private Sector Engagement ..... 2

1.2.4. Engagement with the Public..... 2

1.2.5. Leveraging Cloud and Other Technologies ..... 2

1.2.6. FBI Enterprise Architecture Objectives ..... 2

1.3. Scope ..... 2

1.3.1. Mobile Technologies..... 3

1.3.2. Mobile Applications..... 3

1.3.3. Mobile Infrastructure..... 3

1.4. Intended Audience..... 4

**2. Roles and Responsibilities** ..... 5

2.1. Executive Assistant Director (EAD), Information Technology Branch ..... 5

2.2. Assistant Director (AD), Security Division (SecD)..... 6

2.3. Systems Owners ..... 6

2.4. Mobility Program Office (MPO), Collaboration and Compliance Section (CCS), Information Technology Infrastructure Division (ITID) ..... 7

2.5. Section Chief (SC) of the Information Assurance Section, Security Division .... 7

2.6. Assurance Management Unit, Information Assurance Section, Security Division ..... 7

2.7. Enterprise Security Operations Center, Information Assurance Section, Security Division..... 7

2.8. Information Assurance Technology Unit (IATU), Information Assurance Section, Security Division ..... 8

2.9. Career Services Management Unit (CSMU), Mission Support Section (MSS), Security Division ..... 8

2.10. Physical Security Unit, Security Operations Section (SOS), Security Division.. 8



**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

2.11. Accounts Receivable Unit (ARU), Accounting Section (AS), Finance Division 8

2.12. Asset Management Unit, Accounting Section, Finance Division ..... 8

2.13. Procurement Section, Finance Division ..... 9

2.14. Insider Threat Center, Inspection Division ..... 9

2.15. Internal Investigations Section, Inspection Division..... 9

2.16. FBI Accessibility Program, Product Assurance Unit (PAU), Business Relationship Management Section (BRMS), Information Technology Customer Relationship and Management Division (ITCRMD)..... 9

2.17. Digital Forensics and Analysis Section (DFAS), Operational Technology Division (OTD) ..... 9

2.18. Technically Trained Agent Operations and Development Unit (TODU), Technical Programs Section (TPS), Operational Technology Division ..... 10

2.19. Training Coordination and Support Unit (TCSU), Curriculum Management Section (CMS), Training Division ..... 10

2.20. Creative Media Development Unit (CMDU), Curriculum Management Section, Training Division ..... 10

2.21. Office of the General Counsel..... 10

2.22. Program Manager..... 10

2.23. Division or Field Office Heads ..... 10

2.24. Mobility Point of Contact..... 11

2.25. Enterprise Requirements and Capabilities Working Group (ERC-WG) ..... 11

2.26. Information Technology Portfolio Manager (ITPfm)..... 11

2.27. Property Custodian..... 11

2.28. Chief Security Officer (CSO)..... 12

2.29. FBI Personnel..... 12

3. Policies..... 14

3.1. Mobile Device Entry and Use in FBI-Controlled Facilities..... 14

3.2. FBI-Owned Mobile Devices ..... 14

3.3. Non-FBI-Owned Mobile Devices ..... 14

    3.3.1. Personally Owned Mobile Devices..... 14

    3.3.2. Other Government Agency-, Contractor-, and Vendor-Owned Mobile Devices..... 14

3.4. Installation and Use of Signal Enhancement Devices..... 15

3.5. Security Incidents..... 15

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

3.6. Search and Seizure ..... 15

3.7. Policy Compliance ..... 17

4. Procedures and Processes..... 18

4.1. Entry and Use of Mobiles Device in FBI-Controlled Facilities..... 18

4.1.1. Red/Black Separation..... 18

4.1.2. Other Government Agency-Owned Laptops in FBI-Controlled Facilities .  
..... 19

4.1.3. Mobile Devices in Undercover Locations..... 19

4.2. Remote Access to FBI Information Systems from Mobile Devices ..... 19

4.3. Use of FBI-Owned Mobile Devices ..... 19

4.3.1. Training ..... 19

4.3.2. Appropriate and Responsible Use..... 20

4.3.3. Voice and Data Consumption ..... 21

4.3.4. Use of Mobile Device Accounts ..... 22

4.3.5. Use of Mobile Applications ..... 23

4.3.6. Use of Removable Media ..... 25

4.3.7. Use with Other Information Technology Devices ..... 25

4.3.8. Use of FBI-Owned Mobile Devices While Operating Government  
Vehicles..... 29

4.3.9. Transport and Storage ..... 29

4.3.10. Foreign Travel ..... 30

4.3.11. Software and Hardware Installation or Modification..... 33

4.3.12. Issuance, Maintenance, and Replacement of FBI-Owned Mobile Devices  
33

4.3.13. Device Return..... 34

4.4. Management and Configuration of FBI-Owned Mobile Devices ..... 34

4.4.1. Acquisition ..... 34

4.4.2. Section 508..... 34

4.4.3. Asset Management ..... 35

4.4.4. Security Assessment and Authorization..... 35

4.4.5. Marking ..... 35

4.4.6. Configuration ..... 35

**UNCLASSIFIED**

**Mobile Devices and Mobile Applications Policy Guide**

4.4.7. Encryption ..... 36

4.4.8. Malware Protection ..... 36

4.4.9. Service Management ..... 36

4.4.10. Mobile Application Management..... 36

4.4.11. Mobile Infrastructure..... 37

4.4.12. Foreign Travel Device Configuration ..... 37

4.4.13. Remote Administration ..... 38

4.4.14. Collection of Data Analytics ..... 39

4.4.15. Sanitization and Destruction ..... 39

4.5. Exemptions and Exceptions ..... 39

5. Summary of Legal Authorities ..... 40

5.1. Federal ..... 40

5.2. Intelligence Community Directives (ICD)..... 40

5.3. Committee on National Security Systems (CNSS) ..... 40

5.4. Department of Justice..... 40

6. Recordkeeping Requirements..... 41

**List of Appendices**

*Appendix A: Final Approvals ..... A-1*

*Appendix B: Sources of Additional Information ..... B-1*

*Appendix C: Contact Information ..... C-1*

*Appendix D: Definitions and Acronyms ..... D-1*

*Appendix E: Security Controls Policy Reference Matrix ..... E-1*

**List of Tables**

**Table 1: Provisions for the Entry and Use of All Mobile Devices in  
FBI-Controlled Facilities ..... 18**

**Table 2: Connection of Unclassified FBI-Owned Mobile Devices to  
Non-FBI-Owned IT Resources ..... 27**

**Table 3: Connection of Unclassified FBI-Owned Mobile Devices to other  
Unclassified FBI-Owned IT Resources ..... 29**

## 1. Introduction

---

### 1.1. Purpose

The purpose of this policy guide (PG) is to establish the minimum requirements for:

- Using mobile devices in compliance with applicable laws, statutes, and regulations, as that use relates to Federal Bureau of Investigation (FBI) operations, internal FBI policies, the *Domestic Investigations and Operations Guide (DIOG)*, or any other applicable or successor documents.
- Safeguarding United States government information (USGI) that is processed, stored, or transmitted on authorized mobile devices.
- Developing, deploying, and using mobile applications (apps) on FBI-owned mobile devices.
- Designing and architecting mobile infrastructure associated with FBI-owned mobile devices, including the services that manage, deliver, exchange, or otherwise control the content and functionality of the devices.

### 1.2. Background

The FBI's mission of protecting the American people and upholding the Constitution of the United States requires an advanced, contemporary, mobile environment to support its workforce. Technology enablement will not only improve the agility and efficiency of FBI personnel in achieving this mission, but it will also enhance the experience of FBI personnel by reducing administrative barriers; facilitating collaboration; and increasing employee recruitment, retention, and satisfaction. A well-developed mobile environment will also benefit the FBI by reducing facility costs, expanding global access to FBI networks, improving Intelligence Community (IC) and law enforcement partnerships, and generally streamlining resource management. It is essential that the FBI keep abreast of commercial technologies, while simultaneously maintaining a balance between information confidentiality, integrity, and availability.

#### 1.2.1. Accountability and Waste Prevention

Two of the primary objectives of this PG are to promote accountability and prevent waste of government resources in accordance with *Executive Order (EO) 13589, Promoting Efficient Spending*. Through sophisticated tracking mechanisms and well-structured user guidance, the FBI aims to detect, reduce, and prevent the wasteful or inappropriate use of government property and/or time.

#### 1.2.2. Intelligence and Law Enforcement Community Engagement and Leadership

Mobile technologies advance the FBI's mission of providing leadership and criminal justice services to federal, state, municipal, and international agencies and partners. Not only does the sharing of advanced technologies improve communication and collaboration between the FBI and its law enforcement and Intelligence Community (IC)

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

partners, it also improves the criminal justice system as a whole by making advanced technologies available to agencies that might otherwise not have access to the same. As a result, the entire criminal justice system is better equipped to address high-impact and time-sensitive crises.

#### **1.2.3. Private Sector Engagement**

The FBI benefits significantly from an increased use of commercially available technologies and strong relationships with leaders in the private technology industry. Meaningful private sector engagement reduces barriers to cooperation and reporting; improves its awareness of, and involvement in, industry innovations; provides higher quality services to its end users; creates preexisting agency-industry communication channels that can be used in the event of emergencies; gives all parties opportunities to share best practices; and nurtures the sharing of ideas and collaboration among personnel.

#### **1.2.4. Engagement with the Public**

The proliferation of commercially available mobile technologies is changing how the American public expects to consume federal government services. Rather than using traditional technology and information sources to learn about and/or contact the FBI, the American public is increasingly turning to mobile technologies through mobile apps, smart phone videos, or similar technologies. As a result, the FBI is becoming more accessible to its primary stakeholders. Mobile technologies also provide the FBI with a nontraditional avenue for public outreach. The FBI is able to access a much broader population in a shorter period of time with minimal strain on its resources. Whether mobile technologies are used as a means for the public reaching the FBI or the FBI reaching the public, they improve the FBI's communication with the American people, which in turn improves the perception of, and experience with, the FBI.

#### **1.2.5. Leveraging Cloud and Other Technologies**

Leveraging cloud and other technologies simultaneously supports the FBI's objectives of modernization and fiscal accountability. The FBI can alleviate physical, financial, and capability limitations on its information technology (IT) workforce and infrastructure by relying on secure and affordable commercial offerings as they become available.

#### **1.2.6. FBI Enterprise Architecture Objectives**

The development, deployment, and use of FBI-owned mobile devices and technologies aligns with the FBI's enterprise architecture objectives, including but not limited to the *Information and Technology Branch (ITB) Enterprise Mobility Strategy* or any of its successor documents.

### **1.3. Scope**

For the purposes of this PG, mobile devices are portable computing devices, such as smart phones, tablets, laptops, and wearables that:

- Are physically small and can be carried easily by a single individual.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- Are designed to operate without a physical connection (e.g., wirelessly transmit or receive information).
- Possess local, nonremovable data storage.
- Are powered-on for extended periods with a self-contained power source.

This PG addresses the entry and use of all mobile devices in FBI-controlled facilities and the deployment and use of FBI-owned mobile devices to process, store, or transmit USGI intended for overt operations, regardless of location within or outside of FBI-controlled facilities.

This PG does not address mobile devices intended for covert operations, bring-your-own-device (BYOD) practices (e.g., personally owned mobile devices used to process, store, or transmit USGI), or exemplars used exclusively to support research and/or digital evidence forensic examinations.

#### **1.3.1. Mobile Technologies**

Mobile technologies addressed by this PG include:

- Enterprise mobile devices issued by the ITB that process, store, or transmit USGI. This does not include preproduction devices used in the design, development, and testing processes.
- FBI-owned mobile devices that process, store, or transmit USGI and were acquired for operational use with operational funds.

#### **1.3.2. Mobile Applications**

Mobile apps addressed by this PG include commercial, custom, and other government agency (OGA)-approved mobile apps developed, deployed, and/or used on FBI-owned mobile devices.

#### **1.3.3. Mobile Infrastructure**

The mobile infrastructure is a comprehensive hosting environment for mobile services that provides the following functions:

- Mobile device management (MDM) or a successor service
- Mobile application management (MAM) or a successor service
- Mobile backend as a service (mBaaS)
- Application program interface (API) or successor service
- Computing, storage, and analytics-enabling content provided to end-user devices

Mobile infrastructure addressed by this PG include physical and virtual infrastructure for FBI-owned mobile services, including cloud-hosted and privately hosted services.

## **UNCLASSIFIED**

### Mobile Devices and Mobile Applications Policy Guide

#### **1.4. Intended Audience**

This PG applies to all FBI personnel who use or possess FBI-owned mobile devices, any individuals bringing non-FBI owned mobile devices into FBI-controlled facilities, any individuals possessing non-FBI owned mobile devices while in FBI-controlled facilities, and all FBI personnel and entities responsible for the development, deployment, and management of FBI-owned mobile devices and technologies used for overt purposes.

## 2. Roles and Responsibilities

---

### 2.1. Executive Assistant Director (EAD), Information Technology Branch

The EAD of ITB (or designee) must ensure that:

- Procedures and processes are established for the acquisition and asset management of FBI-owned mobile devices, in coordination with the Procurement Section of the Finance Division (FD) and the Asset Management Unit of FD.
- The makes and models of FBI-owned mobile devices approved for acquisition are maintained and updated on the FBI Standard Products List (SPL).
- Approval decisions for exemption requests regarding the acquisition of FBI-owned mobile devices are made in coordination with the Procurement Section of FD.
- Approval decisions for exemption requests regarding the asset management of FBI-owned mobile devices are made in coordination with the Asset Management Unit of FD.

As the FBI authorizing official, the EAD of ITB (or designee) must:

- Make approval decisions, in coordination with systems owners, for sharing FBI-owned mobile devices between FBI personnel.
- Make approval decisions for all connections of mobile devices to FBI information systems or resources.
- Designate personnel to establish and publish a process for the custom development or acquisition of mobile apps for FBI-owned mobile devices.
- Make approval decisions for all mobile apps used with FBI-owned mobile devices.
- Make approval decisions regarding deviations from the requirements described in this PG for FBI-owned mobile devices.
- Review waiver requests regarding (1) foreign travel with FBI-owned laptops and (2) foreign travel with all other FBI-owned mobile devices to high- or critical-threat countries.
- Make approval decisions regarding foreign travel with FBI-owned mobile devices (other than laptops) to low- or moderate-threat countries.
- Submit waiver requests regarding (1) foreign travel with FBI-owned laptops and (2) foreign travel with all other FBI-owned mobile devices to high- or critical-



## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

threat countries to the Department of Justice (DOJ) chief information security officer (CISO) for approval decisions.

#### **2.2. Assistant Director (AD), Security Division (SecD)**

The AD of SecD must ensure that:

- The security requirements of this PG are supported through FBI security programs.
- The security violations of this PG are investigated and sanctions are enforced, when appropriate.

#### **2.3. Systems Owners**

Systems owners for any FBI-owned mobile device must ensure that:

- FBI-owned mobile devices meet the requirements described in this PG.
- The appropriate usage criteria for FBI-owned mobile devices are defined.
- The approval decisions for sharing FBI-owned mobile devices between FBI personnel are made in coordination with the FBI authorizing official are made.
- The rules of behavior for FBI-owned mobile devices are developed and maintained in coordination with the Information Assurance Section (IAS) of SecD and the Office of the General Counsel (OGC).
- Procedures and processes are established for managing and tracking the issuance of FBI-owned mobile devices to FBI personnel.
- Training regarding system-specific procedures and processes, including, at a minimum, appropriate usage and rules of behavior, is provided to FBI personnel upon receipt of FBI-owned mobile devices.
- Criteria are established for FBI personnel to maintain FBI-owned mobile devices when transferring within the FBI.
- Procedures and processes are established, in coordination with the Enterprise Security Operations Center (ESOC) of SecD and with OGC, for requesting, vetting, and approving mobile apps used with FBI-owned mobile devices.
- Procedures and processes are established for reviewing voice and data usage and additional charges incurred by users of FBI-owned mobile devices.
- Logs of FBI personnel with a history of overuse are maintained.
- Security monitoring for FBI-owned mobile devices is performed in coordination with the ESOC of SecD.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- Procedures and processes are established for analyzing FBI-owned mobile devices for potential compromise and for performing firmware restoration.
- Procedures and processes are established for handling security incidents involving FBI-owned mobile devices and any associated information-storage capabilities (e.g., server or cloud computing provider/service) and are approved by the FBI authorizing official.
- Procedures and processes are established for capturing and maintaining records created on FBI-owned mobile devices.
- Procedures and processes are implemented to protect and preserve information stored on FBI-owned mobile devices during investigations of unauthorized or inappropriate use.

#### **2.4. Mobility Program Office (MPO), Collaboration and Compliance Section (CCS), Information Technology Infrastructure Division (ITID)**

The MPO must perform the system-owner responsibilities for enterprise mobile devices, as assigned by the FBI CIO.

#### **2.5. Section Chief (SC) of the Information Assurance Section, Security Division**

The SC of IAS must make approval decisions for exemption requests related to the entry and use of mobile devices in FBI-controlled facilities and must coordinate with other sections within SecD, as necessary.

#### **2.6. Assurance Management Unit, Information Assurance Section, Security Division**

The Assurance Management Unit of SecD must:

- Identify, publish, and maintain restrictions regarding the entry and use of mobile devices in FBI-controlled facilities.
- Provide security input to systems owners regarding the rules of behavior for FBI-owned mobile devices.
- Develop and update security awareness training regarding mobile devices, at least annually, in coordination with the Career Services Management Unit (CSMU) of SecD. This training may be combined with the annual security awareness training or other training, as deemed appropriate by the Training Division (TD).
- Perform a compliance assessment in accordance with the *Information Assurance (IA) Policy Compliance Assessment Plan*.

#### **2.7. Enterprise Security Operations Center, Information Assurance Section, Security Division**

The ESOC must ensure that:

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- A security review of mobile apps used with FBI-owned mobile devices is provided.
- Procedures and processes are established for monitoring unauthorized and inappropriate use of FBI-owned mobile devices, in coordination with the Insider Threat Center (InTC) and the Internal Investigations Section (IIS) of the Inspection Division (INSD).
- Security monitoring for FBI-owned mobile devices is performed in coordination with systems owners.

#### **2.8. Information Assurance Technology Unit (IATU), Information Assurance Section, Security Division**

The IATU of SecD must make recommendations to the Physical Security Unit (PSU) of SecD regarding the installation and use of signal-enhancement devices in FBI-controlled facilities or on FBI-controlled property.

#### **2.9. Career Services Management Unit (CSMU), Mission Support Section (MSS), Security Division**

The CSMU of SecD must develop and update security awareness training regarding mobile devices, at least annually, in coordination with the IAS of SecD. This training may be combined with the annual security awareness training or other training, as deemed appropriate by TD.

#### **2.10. Physical Security Unit, Security Operations Section (SOS), Security Division**

The PSU of SecD must make approval decisions regarding the installation and use of signal enhancement devices in FBI-controlled facilities or on FBI-controlled property.

#### **2.11. Accounts Receivable Unit (ARU), Accounting Section (AS), Finance Division**

The ARU of FD must:

- Process any payments received from FBI personnel, FBI Headquarters (FBIHQ) divisions, or field offices (FO) for unauthorized charges incurred by users of enterprise mobile devices and apply them to costs directly associated with the MPO.
- Track and report receipt of payments for unauthorized charges incurred by users of FBI-owned mobile devices to the MPO.

#### **2.12. Asset Management Unit, Accounting Section, Finance Division**

The Asset Management Unit of FD, in coordination with the FBI CIO, must:

- Establish and publish procedures and processes for the asset management of FBI-owned mobile devices.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- Make approval decisions for exemption requests regarding the asset management of FBI-owned mobile devices.

#### **2.13. Procurement Section, Finance Division**

The Procurement Section of FD, in coordination with the FBI CIO, must:

- Establish and publish procedures and processes for the acquisition of FBI-owned mobile devices.
- Make approval decisions for exemption requests regarding the acquisition of FBI-owned mobile devices.

#### **2.14. Insider Threat Center, Inspection Division**

The InTC of INSD must:

- Identify and analyze insider threat matters, including the receipt and analysis of relevant data on FBI-owned mobile devices.
- Notify systems owners, as soon as practicable and appropriate, of insider threat concerns that are likely to lead to investigative activity so systems owners may implement procedures and processes to protect and preserve information stored on FBI-owned mobile devices.

#### **2.15. Internal Investigations Section, Inspection Division**

The IIS of INSD must evaluate the unauthorized and inappropriate use of FBI-owned mobile devices by FBI personnel and determine appropriate courses of action.

#### **2.16. FBI Accessibility Program, Product Assurance Unit (PAU), Business Relationship Management Section (BRMS), Information Technology Customer Relationship and Management Division (ITCRMD)**

The FBI Section 508 coordinator of the FBI Accessibility Program must make approval decisions for exemption requests regarding the inability of FBI-owned mobile devices to provide users with disabilities equal or comparable access to, and use of, information and data as users without disabilities.

#### **2.17. Digital Forensics and Analysis Section (DFAS), Operational Technology Division (OTD)**

The DFAS of OTD must:

- Process all digital evidence, including evidentiary mobile technologies, mobile apps, and mobile infrastructure, in accordance with the *Digital Evidence Policy Directive and Policy Guide, 0639DPG*.
- Perform all forensic examinations of FBI mobile technologies, mobile apps, and infrastructure, as described by the *Digital Evidence Policy Directive and Policy Guide, 0639DPG*.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

#### **2.18. Technically Trained Agent Operations and Development Unit (TODU), Technical Programs Section (TPS), Operational Technology Division**

The TODU of OTD must:

- Provide TEMPEST guidance to users for mitigating risks associated with mobile device use in FBI-controlled facilities.
- Make approval recommendations to the PSU of SecD regarding the installation and use of signal enhancement devices in FBI-controlled facilities or on FBI-controlled property.

#### **2.19. Training Coordination and Support Unit (TCSU), Curriculum Management Section (CMS), Training Division**

The TCSU of TD must assist with the development and maintenance of training regarding mobile devices, as necessary.

#### **2.20. Creative Media Development Unit (CMDU), Curriculum Management Section, Training Division**

The CMDU of TD must assist with the development and delivery of mobile apps for FBI-owned mobile devices that are required to address training requirements.

#### **2.21. Office of the General Counsel**

The OGC must:

- Provide legal input to systems owners regarding the rules of behavior for FBI-owned mobile devices.
- Provide a legal and/or privacy review of mobile apps used with FBI-owned mobile devices.

#### **2.22. Program Manager**

Program managers must identify users who must receive FBI-owned mobile devices due to mission requirements.

#### **2.23. Division or Field Office Heads**

Division or FO heads, or designees, must:

- Designate mobility points of contact (POC) to manage the issuance and return of enterprise mobile devices.
- Make approval decisions for users to receive enterprise mobile devices. This approval authority may not be delegated any lower than the unit chief (UC) or supervisor level. Approval for users designated by program managers must also be granted, and devices must not be reassigned absent a compelling reason.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- Make approval decisions for users to incur global charges during the use of their enterprise mobile devices while on foreign travel. This approval authority may not be delegated any lower than the UC or supervisor level.
- Assign appropriate personnel to review (at least monthly) voice and data usage and additional charges incurred by users of enterprise devices.
- Initiate payment requests, upon receiving notification of instances of excessive usage from the MPO, to FBI personnel responsible for incurring unauthorized charges. Division and FO heads may coordinate with their mobility POCs to manage and track these requests.
- Ensure that the mobile telephone numbers (MTN) for users with enterprise mobile devices identified by the MPO as inactive (i.e., no material voice, data, or text-messaging service, such as short messaging service [SMS] or multimedia messaging service [MMS]) for 30 calendar days or more are suspended, removed, revoked, and/or reallocated when maintenance of those lines incurs a cost or when required.

#### **2.24. Mobility Point of Contact**

The mobility POC of a division or an FO must:

- Manage the issuance and return of enterprise mobile devices.
- Maintain completed and signed rules of behavior forms for users of enterprise mobile devices in the official personnel files of those individuals.
- Manage the MTNs of enterprise mobile devices.

#### **2.25. Enterprise Requirements and Capabilities Working Group (ERC-WG)**

The ERC-WG must review product charters for custom mobile apps used with FBI-owned mobile devices and provide approval recommendations to the FBI authorizing official.

#### **2.26. Information Technology Portfolio Manager (ITPfm)**

The ITPfm must review product charters for business functions, including both commercial and custom mobile apps used with FBI-owned mobile devices and must provide approval recommendations to the ERC-WG.

#### **2.27. Property Custodian**

The property custodian of a division or an FO must:

- Meet acquisition and asset management requirements for FBI-owned mobile devices.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- Maintain the receipt of government property forms for users of FBI-owned mobile devices.

#### **2.28. Chief Security Officer (CSO)**

The CSO of a division or an FO must:

- Establish procedures and processes to ensure compliance with this PG for FBI-controlled facilities under his or her purview. The CSO may incorporate additional restrictions into the procedures and processes if necessary.
- Conspicuously post notices regarding the entry and use of mobile devices in FBI-controlled facilities.
- Implement procedures within FBI-controlled facilities under his or her purview to meet red/black separation requirements.
- Make approval decisions for the use of OGA-, contractor-, and vendor-owned mobile devices with FBI IT resources that do not process, store, or transmit USGI.
- Make approval decisions regarding the entry and use of OGA-owned laptops in FBI Sensitive Compartmented Information facilities (SCIF).
- Provide foreign travel briefings to users of FBI-owned mobile devices prior to their travel and foreign travel debriefings upon their return.
- Collect and maintain information, in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and the Americans with Disabilities Act (ADA), regarding FBI personnel who possess medical devices (e.g., hearing aids, pacemakers, and implanted medical devices) containing wireless medical data telemetry, remote control monitoring, or external interface capabilities.
- Implement risk mitigations for FBI personnel who possess medical devices containing wireless medical data telemetry, remote control monitoring, or external interface capabilities.

#### **2.29. FBI Personnel**

All FBI personnel must:

- Request approval from their division or FO heads to receive enterprise mobile devices.
- Complete security awareness trainings regarding mobile devices, when required.
- Read, sign, and abide by the rules of behavior for non-FBI-owned mobile devices prior to bringing them into FBI-controlled facilities.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- Read, sign, and abide by the rules of behavior for FBI-owned mobile devices prior to receiving devices.
- Submit MTN change requests for enterprise mobile devices to mobility POCs.
- Request approval from division or FO heads, prior to foreign travel, to incur global charges during the use of FBI-owned mobile devices while on foreign travel.
- Report travel with FBI-owned mobile devices, prior to foreign travel, in accordance with the process described in Policy Directive (PD) 0329D, *Official Foreign Travel* or PD 0380D, *Unofficial Foreign Travel*, based on the type of travel.
- Provide payment for unauthorized charges incurred during the use of FBI-owned mobile devices to the ARU of FD, when required.
- Return FBI-owned mobile devices to mobility POCs or systems owners upon separation, termination, or when required.
- Notify mobility POCs or systems owners when it is expected that FBI-owned mobile devices will not be used for more than 30 calendar days.
- Notify visitors (non-FBI personnel), prior to arrival, of restrictions regarding the use of mobile devices in FBI-controlled facilities.
- Notify CSOs of medical devices containing wireless medical data telemetry, remote control monitoring, or external interface capabilities prior to entry and use in FBI-controlled facilities.
- Safeguard and protect personally identifiable information (PII) on FBI-owned mobile devices, in accordance with PD 0592, *Encryption of Electronic FBI Information*.



### 3. Policies

---

#### 3.1. Mobile Device Entry and Use in FBI-Controlled Facilities

In order to protect intelligence, national security, and law enforcement information processed, stored, and transmitted in FBI-controlled facilities, the entry and use of all mobile devices within FBI-controlled facilities must be performed in accordance with all security requirements and procedures identified in this PG (see [subsection 4.1.](#)).

#### 3.2. FBI-Owned Mobile Devices

Users of FBI-owned mobile devices, including enterprise and operational, devices must comply with all security, training, acquisition, asset management, service management, appropriate and responsible use, MAM, and mobile infrastructure requirements and procedures identified in this PG (see [subsections 4.2.](#) and [4.3.](#)).

#### 3.3. Non-FBI-Owned Mobile Devices

Users of non-FBI-owned mobile devices must comply with the requirements described below. Non-FBI-owned mobile devices that do not meet one of the ownership categories described in this section are considered personally owned.

##### 3.3.1. Personally Owned Mobile Devices

Generally, personally owned mobile devices must not be used to conduct official FBI business. This includes processing, storing, or transmitting USGI. Permissible exceptions to this rule are as follows:

- Limited voice and/or data usage of a personally owned mobile device for conducting unclassified, nonsensitive, official FBI business when the use of an FBI-owned mobile device is not possible or practicable. Examples include, but are not limited to:
  - Coordinating nonoperational meeting information.
  - Using Global Positioning Satellite (GPS) for navigation or directions.
  - Locating FBI personnel and communicating continuity of operations [COOP] plans during or after a natural disaster.
- Use of a personally owned mobile device for accessing the Unclassified Network (UNet) Outlook Web Application (OWA). See [subsection 4.2.](#) for more information regarding remote access.

Personally owned mobile devices must not be connected to, or used with, FBI IT resources unless approved by the FBI authorizing official.

##### 3.3.2. Other Government Agency-, Contractor-, and Vendor-Owned Mobile Devices

OGA-owned mobile devices are prohibited from use with FBI IT resources that process, store, or transmit USGI without the following:

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- Approval from the OGA authorizing official
- Approval from the FBI authorizing official through the security assessment and authorization (SAA) process described in the *Security Assessment and Authorization Policy Guide, 0655PG*
- An approved memorandum of understanding (MOU), a memorandum of agreement (MOA), or an interconnection security agreement (ISA), when required

The affected chief division counsel (CDC) or OGC must be consulted to determine when an MOU, an MOA, or an ISA is required, in accordance with the *FBI Memorandum of Understanding and Non-Contractual Agreements Policy Guide, 0273PG*. If approved, OGA-owned mobile devices must be used in accordance with the requirements for FBI-owned mobile devices.

Contractor-owned and vendor-owned mobile devices are also prohibited from use with FBI IT resources that process, store, or transmit USGI without the following:

- Approval from the FBI authorizing official through the SAA process described in the *Security Assessment and Authorization Policy Guide, 0655PG*
- An approved contract agreement or statement of work

If approved, contractor-owned and vendor-owned mobile devices must be used in accordance with the requirements for FBI-owned mobile devices.

OGA-, contractor-, and vendor-owned mobile devices are prohibited from use (without approval from the CSO) with FBI IT resources that do not process, store, or transmit USGI.

#### **3.4. Installation and Use of Signal Enhancement Devices**

The installation and use of signal enhancement devices is prohibited in FBI-controlled facilities or on FBI-controlled property without approval from the PSU and requires concurrence from the IATU and TODU.

#### **3.5. Security Incidents**

Known or suspected security incidents must be reported in accordance with the requirements described in the *Security Compliance Program PG, 0934PG*.

A process must be established by systems owners for handling security incidents involving information spillage on mobile devices and associated mobile infrastructure. The process must be identified in the system security plan (SSP) and approved by the FBI authorizing official in accordance with the requirements described in the *Incident Response for FBI Information Systems, 0924PG*.

#### **.Search and Seizure**

As a general rule, governmental searches and seizures conducted without warrants are presumptively unlawful. There are, of course, exceptions to the warrant requirement, but 4th Amendment compliance always requires fact-intensive analysis.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

All FBI-owned mobile devices are potentially subject to search and seizure pursuant to governing laws; regulations; forms and policies; the FD-889b, "Rules of Behavior Agreement for Unclassified FBI Owned Smartphone and Tablet Devices"; and the FD-1001, "Consent for Warrantless Searches of Department of Justice Workplaces."

Generally, searches and seizures of non-FBI-owned mobile devices brought into FBI-controlled facilities must be supported by appropriate warrants or court orders. There may, however, be circumstances in which warrantless searches are appropriate, including, but not limited to, situations where both probable cause and exigent circumstances exist at the same time, or voluntary consent is deemed to have been granted through the FD-889e, "Rules of Behavior Agreement for Non-FBI Owned Mobile Devices." and the FD-1001, "Consent for Warrantless Searches of Department of Justice Workplaces."

Due to the complexity that attends the search and seizure of mobile devices, FBI personnel must consult with their respective CDCs or with OGC, whenever feasible, to determine if a given warrantless search and seizure of any mobile device in FBI-controlled facilities complies with the 4th Amendment. All requests for search authority under the FD-1001 must be coordinated with the Counterintelligence Division, Counterespionage Section, CD-4D. For additional guidance as to searches and seizures, please see DIOG subsections 18.6.12 and 18.7.1.

As a general rule, and absent exceptional circumstances, only sworn law enforcement officers should seize mobile devices. All searches of mobile devices must be conducted or supervised by a sworn law enforcement officer.

The search and examination of a mobile device must adhere to the procedures listed in the Digital Evidence Policy Directive and Policy Guide, 0639DPG.

If USGI including classified, ~~For Official Use Only (FOUO), and Law Enforcement Sensitive (LES) information~~ is discovered to be present on any personally owned or FBI-owned mobile device without approval, a security incident must be reported and handled in accordance with the Security Compliance Program PG. 0934PG. Based upon the classification or sensitivity level of the information, the device may also be sanitized in accordance with PD 0506D, Destruction of Classified and Sensitive Material.

1. If USGI can be effectively and technically removed prior to returning the device to the owner, such efforts must be attempted; however, the owner must be advised in advance that removal techniques may either render the mobile device inoperable or result in the deletion or damage to all information on the device.
2. In other cases, due to classification or sensitivity issues, the device may not be able to be safely returned to the owner. In these cases, the FBI may be able to transfer nonprohibited personal data to a new piece of media; however, the FBI's ability to provide this option will be determined by the assistant SC of DFAS or the FO computer analysis response team (CART) supervisor.

All visitors must be given the option of locking and storing their devices upon entering FBI-controlled facilities.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

#### 3.6. Policy Compliance

Noncompliance with this PG must be reported in accordance with the requirements described in PD 0796D, Reporting FBI Employee Misconduct and PD 0727D, Non-Retaliation for Reporting Compliance Risks. FBI personnel who do not comply with the requirements set forth in this PG may be subject to administrative, criminal, security, or other adverse action.

FBI information systems not in compliance with the security requirements set forth in this PG may be subject to a review and/or revocation of their security authorization to operate (ATO), in accordance with the requirements described in Security Assessment and Authorization Policy Guide, 0655PG.

To ensure compliance with the requirements set forth in this PG, and in accordance with the Information Assurance (IA) Policy Compliance Assessment Plan, a policy compliance assessment must be performed by the IAS at least every two years.

## 4. Procedures and Processes

The procedures and processes described in this section explain how to implement the policy requirements described in Section 3.

### 4.1. Entry and Use of Mobiles Device in FBI-Controlled Facilities

The provisions in Table 1 (below) apply to the entry and use of all mobile devices in FBI-controlled facilities.

Mobile Device Types	Entry and Use in FBI Secret Facilities (with Notes)	Entry and Use in FBI SCIFs (with Notes)
Mobile devices with wireless, speakerphone, photographic, audio/video recording, or video call/chat capabilities	Limited <sup>1,2,3,4,5</sup>	No <sup>3,4,5,6,7,8</sup>
Mobile devices without wireless, speakerphone, photographic, audio/video recording, or video call/chat capabilities	Yes	Yes <sup>8</sup>
<p>Notes</p> <p>1: Wireless (e.g., wireless fidelity [Wi-Fi], Bluetooth, near-field communication [NFC]) capabilities must be disabled prior to entry. Mobile devices incapable of disabling wireless capabilities are prohibited from entry. Use of cellular and infrared capabilities is allowed.</p> <p>2: Use of speakerphone, photographic, audio/video recording, or video call/chat capabilities on non-FBI-owned mobile devices is prohibited.</p> <p>3: Use of photographic, audio/video recording, or video call/chat capabilities on FBI-owned mobile devices is prohibited. Use of speakerphone capabilities on FBI-owned mobile devices may be used in closed conference rooms or private offices. See PD 0627D, <i>Video and Audio Teleconferencing (VTC)</i>.</p> <p>4: Medical devices (e.g., hearing aids, pacemakers, or implanted devices) with wireless data telemetry, remote control monitoring, or external interface capabilities that have been determined to be required by a licensed physician are allowed; however, FBI personnel must notify their CSOs prior to entry and use.</p> <p>5: Visitors must be notified of mobile device provisions prior to their arrival.</p> <p>6: In the event of a natural disaster or a hostile action (e.g., terrorist attack, riot, or civil uprising), FBI-owned wireless radios are allowed during emergency situations.</p> <p>7: FBI- and OGA-owned laptops are allowed; however, wireless capabilities must be disabled prior to entry, and the use of speakerphone, photographic, audio/video recording, video call/chat, or cellular capabilities is prohibited. Use of infrared capabilities is allowed.</p> <p>8: OGA-owned laptops must be approved by the appropriate CSO prior to entry and use. See subsection 4.1.2. regarding approvals.</p>		

**Table 1: Provisions for the Entry and Use of All Mobile Devices in FBI-Controlled Facilities**

#### 4.1.1. Red/Black Separation

Mobile devices approved for entry in FBI-controlled facilities must be kept away from FBI information systems, in accordance with the red/black separation requirements

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

described in Committee on National Security Systems Advisory Memorandum (CNSSAM) TEMPEST/01-13, RED/BLACK Installation Guidance (links to a U//~~FOUO~~ document) and additional guidance, as provided by the TODU.

**4.1.2. Other Government Agency-Owned Laptops in FBI-Controlled Facilities**

Requests for the entry and use of OGA-owned laptops in FBI SCIFs must be submitted to the CSO via an FD-1057 “Electronic Communication” (EC), using file number  and must include the following information:

b7E

- Justification for use
- Time period required for the laptop to be used
- Security classification level of information that will be processed, stored, or transmitted on the laptop
- List of FBI and/or OGA information systems where the laptop will be connected (if applicable)

If approved, OGA-owned laptops must be used in accordance with the connection requirements in subsection 3.3.2. and the provisions in subsection 4.1. of this PG.

CSOs must assign personnel to examine FBI- and OGA-owned laptops that have been connected to FBI information systems for unauthorized storage of information and files. Assigned personnel must perform manual target-word searches and reviews of laptop hard-drives prior to allowing their release from FBI-controlled facilities.

**4.1.3. Mobile Devices in Undercover Locations**

b7E

**4.2. Remote Access to FBI Information Systems from Mobile Devices**

Remote access to an FBI information system from a mobile device must be performed in accordance with the requirements described in the Remote Access for General and Privileged Users Policy Guide, 0655PG-4.

**4.3. Use of FBI-Owned Mobile Devices**

FBI personnel must follow the procedures and processes in this section regarding the use of all FBI-owned mobile devices, including all enterprise and operational devices, regardless of their location within or outside of FBI-controlled facilities.

**4.3.1. Training**

FBI personnel being issued FBI-owned mobile devices must complete training, at least annually, that includes the following:

- Mobile device and mobile app security awareness

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- Appropriate mobile device and mobile app usage, including guidance on *de minimis* personal use
- Privacy, discovery, and records management

#### **4.3.2. Appropriate and Responsible Use**

FBI personnel being issued FBI-owned mobile devices must read, sign, and agree to abide by the applicable rules of behavior prior to receiving the devices.

FBI-owned mobile devices must not be shared with non-FBI personnel, including family or friends.

Some FBI-owned mobile devices are capable of being shared between FBI personnel, given that systems owners and the FBI authorizing official have approved device sharing, and a separate user account for each assigned individual can be established. Exceptions for community devices, such as informational kiosks, must be requested from systems owners and the FBI authorizing official.

##### **4.3.2.1. De Minimis Personal Use**

Per the Standards of Conduct, “employees shall protect and conserve Federal property and shall not use it for other than authorized activities” (Title 5 Code of Federal Regulations [CFR] § 2635.101(b)(9)). Accordingly, per 5 CFR § 3801.105 and 28 CFR § 45.4, USG property must only be employed for personal use when the related expense to the USG is negligible in cost and time. This accommodates *de minimis* personal use of FBI-owned mobile devices in accordance with the following:

- *De minimis* use of FBI-owned mobile devices during scheduled working hours: Personal use of government time and/or property during an employee’s scheduled working hours may only be authorized if the resulting use:
  1. Involves a negligible expense to the FBI.
  2. Does not adversely affect the performance of official duties.
  3. Is of minimal duration and frequency.
- Noninterference or *de minimis* use of FBI-owned mobile devices during nonscheduled working hours:
  1. Involves a negligible expense to the FBI in cost or time.
  2. Does not adversely affect the performance of official duties.

##### **4.3.2.2. Unauthorized Use**

Even if *de minimis* in nature, use of FBI-owned mobile devices must not be for personal reasons, profit-making, commercial activities, or for purposes that are prohibited or reflect adversely on the FBI (e.g., accessing pornography; promoting supremacist or racist causes, selling products or services online, gambling, or similar activities). Accessing social media on an FBI-owned mobile device is expressly prohibited except

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

for operational purposes, according to the *Social Media and Other Electronic Information Sharing Technologies Policy Directive and Policy Guide, 0579DPG*.

FBI personnel are expected to adhere to the requirements in this PG and those in the *FBI Ethics and Integrity Program Policy Directive and Policy Guide, 0754DPG*, at all times when in control of or using an FBI-owned mobile device.

Similarly, when using FBI-owned mobile devices, FBI personnel must adhere to the Hatch Act requirements set forth in the *FBI Ethics and Integrity Program Policy Directive and Policy Guide, 0754DPG*, regardless of whether such use occurs during their scheduled working hours or not. FBI personnel must be cognizant of the fact that they are considered “further restricted employees” under the Hatch Act and are therefore subject to heightened restrictions when using FBI-owned and personally owned mobile devices.

For additional guidance on Hatch Act requirements when using social media on a personally owned mobile device, refer to the *Social Media and Other Electronic Information Sharing Technologies Policy Directive and Policy Guide, 0579DPG*, and the *Frequently Asked Questions Regarding Social Media and the Hatch Act*.

#### **4.3.3. Voice and Data Consumption**

FBI personnel must use FBI-owned mobile devices in accordance with the voice and data consumption criteria established by systems owners.

##### **4.3.3.1. Voice and Data Consumption on Enterprise Mobile Devices**

For each assigned line under the current contract, and until supersession by a subsequent contract, FBI personnel, per assigned line, per month, are allocated:

- 5 gigabytes (GB) of data consumption.
- A maximum of 300 peak-usage minutes, excluding cell-to-cell calls.

FBI personnel must not exceed these limitations without documented and approved justification per MPO procedures. The MPO will be responsible for monitoring and reporting over usage and under usage of enterprise mobile device services.

##### **4.3.3.2. Overuse of Enterprise Mobile Devices**

If a user substantially exceeds the established voice and/or data allocation, the MPO must notify the division or FO head of the overage. This determination will be made by the MPO based upon a number of factors, including contract terms, the actual cost of the over usage to the government, and the nexus of the activity to a business purpose. If there is no demonstrable operational or security-based justification for the overage, the user will receive a warning after the first overage. If the user incurs a second overage that is not justified by a demonstrable operational or security need, the user may be held responsible for the costs incurred by the government for the unjustified overage identified by the MPO and determined by appropriate division supervisory personnel in the offender’s chain of command. FBI personnel must provide payments to the ARU of FD with any supporting documentation.



**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

FBI personnel expecting to exceed either the 5GB or 300-minute allocation (or any subsequent contractual limits) must provide a demonstrable operational or security need and obtain a supervisor's written approval for the expected overage, via EC, to

[REDACTED] ECs must include notifications to division or FO heads and mobility POCs.

b7E

FBI personnel who incur unexpected overages must submit explanatory ECs to appropriate operational case files, providing operational or security justifications within ten calendar days of the notification of overage. ECs must be approved by supervisors and must include notifications to division or FO heads and mobility POCs. If a supervisor does not approve of the excessive use, the user may appeal to the respective SC or assistant special agent in charge (ASAC) to obtain approval. However, if no approval is granted, the user must document the excessive overage through an EC serialized to [REDACTED] with the approval of the appropriate SC or ASAC and notification to the mobility POC.

**4.3.3.3. Under Use of Enterprise Mobile Devices**

If the MPO identifies the substantial under usage of an enterprise mobile device by an FBI end user, it must inform the division or FO POC of the under usage.

Lines that are not otherwise sequestered for investigation purposes and have been inactive (i.e., no material voice, data, or SMS/MMS) for a period of 30 calendar days after the MPO's under usage notification to the division or FO POC may be suspended (i.e., monthly billing will be held in abeyance while division representatives determine whether there are any special circumstances, such as extended sick leave, military leave, or similar situations that have resulted in zero usage or under usage or whether divisional resources must be realigned). If a line has been inactive for a period of 90 calendar days, the division or FO will be asked to reassign the device in support of mission needs or disconnect the line altogether. Lines that are inactive or suspended for a period of 120 calendar days may be disconnected permanently from the FBI's account, unless there is a demonstrated operational, security, or administrative justification for retaining the line.

**4.3.4. Use of Mobile Device Accounts**

Mobile device accounts are allocated to and for use only by the FBI and are only assigned to individual users and not to groups of users for account sharing.

FBI-associated MTNs and similar lines of communication (e.g., e-mail addresses) must only be used with FBI-owned or FBI-approved devices and accounts. Porting, transferring, or forwarding MTNs or other lines of communication to non-FBI-owned devices or accounts is prohibited (e.g., call forwarding from an FBI-owned mobile phone to a personally owned mobile phone). Similarly, FBI personnel are prohibited from forwarding non-FBI-owned MTNs to FBI-owned mobile devices.

MTNs or other lines of communication must be retained by the FBI for business purposes; they will not be transferred or forwarded to individuals who have separated with, or retired from, the FBI under any circumstances. Similarly, the FBI will not provide assistance with the transfer of contact lists or other data content to the personal

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

devices of individuals who are separating with, or retiring from, the FBI, as this would expend government resources for a nongovernment purpose.

**4.3.5. Use of Mobile Applications**

Mobile apps for FBI-owned mobile devices must be used in accordance with the rules of behavior for the device.

**4.3.5.1. Requesting Mobile Applications for Enterprise Mobile Devices**

Requests for commercial and OGA-authorized mobile apps must be submitted through the approved mobile app request process. Once a request is submitted, the proposed mobile app must go through an automated security scan to identify potential security, privacy, discovery, and/or records management concerns. The results of the automated security scan must be documented, via EC, to case file [REDACTED]. If a proposed mobile app successfully clears the automated scanning process, it is readied for approval and release by the FBI authorizing official or designee. If the automated scan does not satisfy existing thresholds, the mobile app request will advance to a secondary mobile app review performed by the MPO, in conjunction with SecD and OGC. Additional documentation, such as a privacy threshold assessment or a charter, may be required to address potential security, privacy, discovery, and/or records management concerns. Upon completion of the secondary mobile app review, the mobile app will be rejected or approved for release by the FBI authorizing official (or designee).

b7E

Once a commercial or OGA-authorized mobile app is approved for release, the name and description of the mobile app will be circulated to a review group, including personnel from MPO, SecD, and OIC, in order to identify any inappropriate or otherwise unsuitable mobile apps for exclusion from that release cycle. Procedures for this review must be documented by the MPO, via EC, to case file [REDACTED].

b7E

Mobile apps that have been developed by OGAs and are not publicly available may be submitted to a third-party mobile app security evaluator for analysis if the FBI authorizing official or another person designated with release authority provides a signed MOU or a release. If the mobile app is not submitted to a third-party mobile app security evaluation provider, the mobile app will be automatically submitted to the secondary mobile app review process. Upon completion of the secondary mobile app review, the FBI's authorizing official (or designee) will reject or approve the mobile app for release.

Commercial and OGA-authorized mobile apps are not supported by the FBI. Users with support needs must seek assistance from the commercial mobile app provider and not the ITB Help Desk (x1500) or any other FBI entity.

Requests for custom mobile apps require the submission of a documented request and product charter to the MPO, both of which must be documented in case file [REDACTED].

The appropriate ITPfM will review the product charter and, if the ITPfM determines that the mobile app aligns with mission needs, the app will be presented to the enterprise requirements and capabilities working group (ERC-WG) for review and recommendation of approval. With consideration given to the

b7E

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

ERC-WG’s recommendation, the FBI authorizing official (or designee) will reject or approve the mobile app for release. If it is determined that the mobile app addresses a training requirement, the development and delivery of the custom mobile app must be coordinated with the CMDU, TD.

If the MPO determines that a mobile app has not cleared the automated scan and/or a secondary mobile app review is essential for an exigent operational need, the mobile app may be made immediately available to the minimum number of devices necessary to satisfy the exigent need. All exigent releases must be documented with a notification to the FBI authorizing official (or designee) and must provide justification, via EC, to case file [redacted]. No mobile app may be deployed for exigent use for more than 90 calendar days without an affirmative deployment recommendation by a secondary mobile app review or an exemption from the review process, as authorized by the FBI authorizing official and documented by the FBI authorizing official, via EC, to case file [redacted].

b7E

The MPO must present a “terms of use” (ToU) agreement to a user prior to the deployment and installation of a mobile app, notifying the user of any restrictions established during the request process by the “intended use justification” and any conditional comments provided by the FBI authorizing official adjudication. Users wishing to use mobile apps beyond their authorized scopes (as described in the ToU) are required to submit new mobile app requests, providing updated intended use justifications, to receive approval for expansions of scope. Procedures must be instituted, maintained, and regularly reviewed by SecD, in conjunction with the MPO, for the continuous monitoring of approved, released mobile apps for any security vulnerabilities.

**4.3.5.2. Updating Mobile Applications on Enterprise Mobile Devices**

Updates to mobile apps may be provided by the MPO, as needed, and FBI end users will be responsible for installing updates.

If a commercial or OGA-authorized mobile app is no longer being issued updates by the developer and is replaced by a new mobile app, FBI personnel must request the new mobile app from MPO through the approved mobile app request process.

**4.3.5.3. Removing Mobile Applications from Enterprise Mobile Devices**

A mobile app may be removed immediately by the MPO from the FBI white list and FBI-owned devices if a security, operational, or compliance vulnerability has been identified. The FBI authorizing official (or designee) may also require the removal of a mobile app.

**4.3.5.4. Intellectual Property**

Under EO 10096, *Providing for a Uniform Patent Policy for the Government with respect to Inventions made by Government Employees and for the Administration of Such Policy*, and 37 Code of Federal Regulations Part 501, the United States government (USG) may obtain title to any invention, including a mobile app, that is made by an FBI employee (1) during working hours; (2) with a contribution by the government in terms of facilities, equipment, materials, funds, or information, or of time

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

or services of other government employees on official duty; or (3) that bears a direct relation to, or is made in consequence of, the employee's official duties. The controller in the Justice Management Division (JMD), DOJ assesses whether an FBI employee has any intellectual property rights relating to an invention. There are three possible outcomes to the controller's determination of an employee's rights:

1. The government obtains the entire right, title, and interest in and to the invention made by the employee. Under 37 CFR § 501.8, the employee can appeal this determination.
2. The employee retains the entire right, title, and interest in and to the invention, subject to the reservation by the government of a nonexclusive, irrevocable, royalty-free license in the invention with the power to grant licenses for all governmental purposes. Under 37 CFR § 501.8, the employee can appeal this determination. If the controller selects this option but the applicable federal agency does not intend to file a patent application for the invention, then the employee is allowed to retain title to the invention subject to USG's reservation of a license to practice the invention by or on behalf of the government (see 15 United States Code [U.S.C.] § 3710d).
3. The employee retains the entire right, title, and interest in and to the invention and is not required to grant a license to the government.

FBI employees responsible for inventions may be entitled to incentives under 15 U.S.C. § 3710b.

FBI employees who may have intellectual property rights in an intangible must consult with OGC to determine the nature and enforceability of that right.

FBI personnel who are not FBI employees have different rights and responsibilities regarding intellectual property. Those persons must likewise contact OGC to determine the nature and enforceability of their intellectual property rights in inventions of their own designs.

#### **4.3.6. Use of Removable Media**

Removable media (e.g., compact discs [CD]/digital versatile discs [DVD], Universal Serial Bus [USB] drives, memory cards, or Subscriber Identification Module [SIM] cards) must be used with FBI-owned mobile devices in accordance with the requirements described in PD 0247D, *Removable Electronic Storage (RES) Media Protection*.

#### **4.3.7. Use with Other Information Technology Devices**

FBI-owned mobile devices must not be used with other IT devices unless authorized by the FBI authorizing official.

##### **4.3.7.1. Connection of Unclassified Mobile Devices to Non-FBI-Owned Information Technology Resources**

The following table describes the connections of unclassified FBI-owned mobile devices to non-FBI-owned IT resources that have been approved by the FBI authorizing official:

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

Non-FBI-Owned IT Resource	Type of Connection To/From an Unclassified, FBI-Owned Mobile Device			
	Wired (e.g., Ethernet, USB, or Analog Audio)	Wireless (e.g., Wi-Fi, Bluetooth, NFC)	Web-Mediated <sup>1</sup>	VPN
Internet Router	Yes	Limited <sup>2,3</sup>	Yes	No
Desktop	No	No	Yes	No
Printer	No	No	No	No
Non-FBI-Owned IT Resource	Type of Connection To/From an Unclassified, FBI-Owned Mobile Device	Non-FBI-Owned IT Resource	Type of Connection To/From an Unclassified, FBI-Owned Mobile Device	Non-FBI-Owned IT Resource
Smart Phone	No	No	Yes	No
Tablet/Hybrid	No	No	Yes	No
Laptop	No	No	Yes	No
Audio Only (e.g., Speakers or Headphones)	Yes	Limited <sup>3</sup>	Yes	No
<u>Wearables With Memory</u> <sup>4</sup>	No	No	Yes	No
Wearable Without Memory <sup>5</sup>	Yes	Limited <sup>3</sup>	Yes	No
Vehicle (Power/Charge Only)	Limited <sup>6</sup>	No	N/A	N/A
Vehicle (Voice Only)	Limited <sup>6</sup>	Limited <sup>3,6</sup>	Yes	No
Vehicle (Data) (e.g., Text and Contacts Sync)	No	No	Yes	No
Personal Cloud Resource (e.g., Dropbox, Google Drive)	No	No	No	No

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

Notes
1: Web-mediated means accessing information via either Web browser or approved mobile apps to interact with personally owned mobile devices. For example, accessing a home security device's video feed from an FBI-owned mobile device by logging into the security system provider's Web site. These connections generally use Secure Hyper Text Transfer Protocol (HTTPS) or similar security mechanisms.
2: The security setting of the Wi-Fi or hotspot must be at a minimum of Wi-Fi Protected Access II (WPA2) between the device and a known Internet service provider (ISP), without any intermediaries (e.g., FBI personnel must not connect through coffee shop, hotel, or other intermediary that provides unverified Wi-Fi hotspots). Intentionally avoiding this requirement by chaining an FBI-owned device to a personally owned device connected to an unverified Wi-Fi hotspot is prohibited.
3: Connection is permitted outside of FBI-controlled facilities.
4: For example, a smart watch capable of receiving or storing any data from an FBI-owned device would be considered a wearable with memory.
5: For example, a sensor that solely counts steps is wearable without memory.
6: Users must ensure that their devices do not transfer and/or store any information contained on those devices (e.g., data or contacts) to vehicles.

**Table 2: Connection of Unclassified FBI-Owned Mobile Devices to Non-FBI-Owned IT Resources**

FBI personnel are prohibited from using proxies to obscure their personal activities or identities when using FBI-owned mobile devices. A proxy is only allowed when there is an authorized operational need.

FBI personnel are also reminded to ensure that the IT devices with which FBI-owned mobile devices are approved for use do not store USGI or PII in any capacity.

**4.3.7.2. Connection of Unclassified Mobile Devices to Other FBI-Owned Information Technology Resources**

The following table describes the connections of unclassified FBI-owned mobile devices to other unclassified FBI-owned IT resources that have been approved by the FBI authorizing official:

FBI-Owned IT Resource	Type of Connection to/from an Unclassified FBI-Owned Mobile Device			
	Wired (e.g., Ethernet, USB, or Analog Audio)	Wireless (e.g., Wi-Fi, Bluetooth, NFC)	Web-Mediated <sup>1</sup>	VPN
UNet Desktop	Limited <sup>2,3</sup>	No	Yes	No
UNet Laptop	No	No	Yes	No
Cloud Service APIs <sup>4</sup>	No	No	Yes	No
Cloud Desktop via Remote Desktop Protocols (RDP) <sup>5</sup>	No	No	Yes	Yes
Stand-Alone Desktop <sup>6</sup>	Limited <sup>3</sup>	Limited <sup>7</sup>	Yes	Yes

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

Smartphone	Limited <sup>3</sup>	Limited <sup>7</sup>	Yes	No
Wearables <sup>8</sup>	Limited <sup>3</sup>	Limited <sup>7</sup>	Yes	No
Tablet <sup>9</sup>	Limited <sup>3</sup>	Limited <sup>7</sup>	Yes	Yes
Stand-Alone <sup>2</sup> Laptop	Limited <sup>3</sup>	Limited <sup>7</sup>	Yes	Yes

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

Non-FBI-Owned IT Resource	Type of Connection To/From an Unclassified, FBI-Owned Mobile Device			
	Wired (e.g., Ethernet, USB, or Analog Audio)	Wireless (e.g., Wi-Fi, Bluetooth, NFC)	Web-Mediated <sup>1</sup>	VPN

Notes

1. Web-mediated means accessing information via either Web browser or approved mobile apps to interact with personally owned mobile devices. For example, accessing a home security device’s video feed from an FBI-owned mobile device by logging into the security system provider’s Web site. These connections generally use HTTPS or similar security mechanisms.
2. File transfer is allowed for operational purposes if there is no logical connection available.
3. Within FBI-controlled facilities, the device must be in airplane mode or a similar mode that disables wireless capabilities.
4. API describes the controls and data exchange standards necessary to get information and pass information to trusted partners.
5. Remote Desktop Protocols (RDP) encompass the multitude of methods used to access remote services, such as Virtual Desktop Infrastructure (VDI).
6. Stand-alone means the device is not connected to FBI UNCLASSIFIED enclave; however, the device has the ability to be connected to the Internet.
7. Connection is permitted outside of FBI-controlled facilities.
8. Encompasses any peripherals.
9. Includes hybrids such as Surface Pros.

**Table 3: Connection of Unclassified FBI-Owned Mobile Devices to other Unclassified FBI-Owned IT Resources**

**4.3.8. Use of FBI-Owned Mobile Devices While Operating Government Vehicles**

FBI personnel must follow the requirements described in the Government Vehicle Use Policy Guide, 0791PG, for using FBI-owned mobile devices while operating government vehicles.

**4.3.9. Transport and Storage**

FBI personnel are responsible for the security of all FBI-owned mobile devices in their possession to prevent the unauthorized handling of, or access to, FBI-owned mobile devices or information stored thereon. At all times, devices must be in the physical possession and/or physical control of FBI personnel. When devices are not in the physical possession or control of FBI personnel, they must be locked and securely stored to prevent unauthorized handling or access (e.g., USG-approved container/safe/locker, locked vehicle, or residence). Hotel safes must not be used to store devices.

If an FBI-owned mobile device is misplaced, lost, stolen, or handled or accessed by an unauthorized individual for any duration of time, it constitutes a security incident and must be reported in accordance with the process described in Security Compliance Program PG, 0934PG.



## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

#### 4.3.9.1. Transport and Storage of Classified Devices

FBI-owned mobile devices containing classified information must be transported and stored in accordance with the requirements described in *Safeguarding Classified National Security Information Corporate Policy Directive and Policy Implementation Guide (0632DPG)* and the *Courier Program Policy Directive and Policy Guide (0719DPG)*.

#### 4.3.10. Foreign Travel

Users must follow the requirements in this PG when planning personal or business travel to countries outside of the United States and its territories with an FBI-owned mobile device.

Based on the foreign country's threat level, as described in the *FBI Critical and High Threat Country Technical Threat List*, the requirements for foreign travel with an FBI-owned mobile device are divided into the following categories:

- Low- or moderate-threat countries
- High- or critical-threat countries: requirements levied in addition to the requirements for low- or moderate-threat countries

##### 4.3.10.1. Prior to Travel

All foreign travel with FBI-owned mobile devices by FBI personnel must be reported in accordance with the process described in *PD 0329D, Official Foreign Travel*, or *PD 0380D, Unofficial Foreign Travel*, based on the type of travel.

FBI employees, or other FBI personnel when deemed operationally prudent, traveling outside the United States or United States territories must take enterprise mobile devices for personal security, regardless of whether the trip is for personal or official business. The MPO will provide FBI personnel with enterprise mobile devices (if they do not currently have them). In the event that an employee is traveling to a high- or critical-threat country, he or she must consult with the mobility POC to determine the device requirement.

CSOs must ensure that FBI personnel complete foreign travel briefings in accordance with the processes described in *PD 0329D, Official Foreign Travel*, or *PD 0380D, Unofficial Foreign Travel*, based on the type of travel.

##### 4.3.10.1.1. Cellular Service on Enterprise Mobile Devices

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

Prior to FBI personnel going on foreign travel, cellular voice and data services must be switched to an approved international plan. When FBI personnel report their foreign travel, the MPO is automatically notified. FBI personnel are encouraged to verify with the MPO that their plans have been appropriately switched prior to travel.

#### **4.3.10.1.2. External Storage/Removable Media**

For travel to low- or moderate-threat countries, FBI personnel must validate that external storage/removable media is actually required, and it is recommended that the external storage/removable media be removed from devices prior to travel.

In high- or critical-threat countries, the use of external storage/removable media is prohibited, and the media must be removed prior to travel.

#### **4.3.10.2. Use of Devices During Travel**

FBI personnel must follow the requirements in this section when using FBI-owned mobile devices during foreign travel.

##### **4.3.10.2.1. Transport and Storage**

At all times during foreign travel, FBI personnel must keep their FBI-owned mobile devices charged and turned on and must have positive control over their devices, unless there is a demonstrable security or operational need. FBI personnel must not put devices in checked baggage or leave them in unsecured facilities. Hotel safes must not be used as secure storage containers.

FBI personnel are allowed to utilize secure storage containers in USG-controlled and nonpublicly accessible facilities (e.g., embassy, consulate, or military base) to store their devices.

##### **4.3.10.2.2. Device Seizure by Foreign Agents**

FBI personnel must not disclose the passwords of devices to foreign agents, if reasonably allowable. If seizure of equipment or arraignment is threatened, FBI personnel may type in their device passwords and hand the unlocked devices to the agents for inspection. Any passwords to mobile apps installed on phones must not be further disclosed to protect individuals and to prevent the disclosure of USGI.

##### **4.3.10.2.3. Use of Cellular and Wireless Services**

FBI personnel are strongly cautioned to maintain a high level of awareness regarding data usage because high roaming costs may occur when using cellular or data services during foreign travel.

When a device is in use but is not connected to a USG-issued or USG-controlled wireless access point, the device must be placed in airplane mode to prevent potential erroneous transmissions. (A waiver for this requirement is being requested from DOJ, and the requirement will be removed from this policy if the waiver is received.)

For travel to low- or moderate-threat countries:

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

- FBI personnel must not connect devices to public or “shared-key” Wi-Fi networks or hotspots, even if secure protocols like WPA2 may be used. The wide availability of the network or hotspot makes the network insecure (this includes all hotels and coffee shops). The connection of devices to unsecured Wi-Fi connections is strictly prohibited. FBI personnel are permitted to connect devices to USG-furnished Wi-Fi hotspots. In those cases, the security setting of the Wi-Fi or hotspot must be at a minimum of WPA2.
- Other wireless communications, including, but not limited to, Bluetooth and NFC, must be disabled at all times.
- GPS and other location-tracking capabilities must be enabled, unless there is an operational need to disable location services, regardless of the country’s threat level.

For travel to high- or critical-threat countries:

- FBI personnel must only connect devices to Wi-Fi networks or hotspots controlled and maintained by the USG where the security setting is at a minimum of WPA2.
- All wireless communications, including, but not limited to, Bluetooth, NFC, and GPS capabilities, must be disabled at all times. (A waiver for this requirement is being requested from DOJ, and the requirement will be removed from this policy if the waiver is received.)

#### **4.3.10.2.4. Mobile App Store**

FBI personnel must not download, install, or update mobile apps from public and/or private mobile app stores while on foreign travel, unless directed by systems owners.

#### **4.3.10.2.5. Over-the-Air (OTA) Device Updates**

FBI personnel must not perform OTA firmware updates to their devices (or operating systems) while on foreign travel, unless stationed outside the continental United States (OCONUS) or otherwise directed by systems owners.

#### **4.3.10.2.6. Use with Other Information Technology Devices**

FBI personnel must not connect FBI-owned mobile devices to any devices that are not FBI-owned or otherwise approved by systems owners (e.g., public computer, public wall charger, or airport charger) for data transfer or power charging.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

#### 4.3.10.2.7. Incident Reporting

FBI personnel must follow the procedures described in Security Compliance Program PG. 0934PG, for reporting any security incidents or unusual activity that occurred during their travel. Any incident that occurs during foreign travel must be reported by the user to his or her CSO within the following timelines:

- Low- or moderate-threat countries: within the timelines described in Security Compliance Program PG. 0934PG
- High- or critical-threat countries: within 60 minutes of discovery

Examples of incidents requiring reporting include, but are not limited to:

- A foreign agent requests or forces temporary or permanent forfeiture of a device.
- Potential password compromises.
- Device loss: If a device was left in a taxi, for example, communicating first with the taxi company/concierge to retrieve the device would be an appropriate first step; however, this must be reported.
- Device misplacement: If a device was misplaced, but is believed to be among a user's belongings (e.g., hotel room), this must be reported.
- Unknown mobile apps appear to have been installed on a device.

#### 4.3.10.3. Following Travel with FBI-Owned Mobile Devices

Following foreign travel with FBI-owned mobile devices, FBI personnel must complete foreign travel debriefings in accordance with PD 0329D, *Official Foreign Travel*, or PD 0380D, *Unofficial Foreign Travel*, based on the type of travel.

##### 4.3.10.3.1. Following Travel with Enterprise Mobile Devices

Following foreign travel with enterprise mobile devices, FBI personnel must complete foreign travel debriefings that provide automatic notifications to the MPO so that devices can be removed from their international plans and returned to their original domestic plans.

FBI personnel must also exchange or return devices to their mobility POCs when returning from high- or critical-threat countries.

#### 4.3.11. Software and Hardware Installation or Modification

FBI personnel must not install or modify software or hardware on FBI-owned mobile devices without approval from systems owners. The unauthorized installation or modification of software or hardware on FBI-owned mobile devices constitutes a security incident and must be reported in accordance with the process described in Security Compliance Program PG. 0934PG.

#### 4.3.12. Issuance, Maintenance, and Replacement of FBI-Owned Mobile Devices

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

FBI personnel must follow the issuance and replacement procedures established by systems owners for FBI-owned mobile devices.

**4.3.12.1. Issuance, Maintenance, and Replacement of Enterprise Mobile Devices**

The MPO must maintain an ongoing inventory of all enterprise devices and track to whom they are assigned.

Incoming special agents (SA), IAs, and mobile surveillance teams (MST) must be assigned enterprise mobile devices during initial training. All FBI personnel assigned enterprise mobile devices must retain those devices, or their logical replacement(s), throughout their employment, including reassignments, as long as they are in positions that require them to have the devices. Enterprise mobile devices must not be reassigned by FBIHQ division or FO heads absent a compelling reason.

If an FBIHQ division/FO head chooses to reassign an enterprise mobile device, the compelling reason must be documented, via EC, to the MPO Sentinel subfile

[redacted] In the event an SA, an IA, or an MST device is reassigned, the enterprise mobile device must be reassigned to an individual in the same job series.

b7E

In the event FBI personnel need to replace or have maintenance performed on existing devices, they must contact the appropriate mobility POC. If a device is repaired or replaced, the mobility POC will be responsible for submitting an EC to

[redacted] for every replacement device issued. The EC must be approved by the requesting individual's supervisor, and he or she must contact the appropriate mobility POC. If a device is repaired or replaced, the mobility POC will be responsible for submitting an EC to the requesting individual's supervisor (with the MPO on the distribution list) for approval.

**4.3.13. Device Return**

FBI personnel must follow appropriate return procedures for all FBI-owned devices in the event of separation, suspension, retirement, extended leave, or temporary duty (TDY) assignment to an OGA. See PD 0304D, Return of Government Property Upon Separation from the FBI.

**4.4. Management and Configuration of FBI-Owned Mobile Devices**

FBI personnel must follow the procedures and processes in this section regarding the management of FBI-owned mobile devices, including enterprise and operational devices.

**4.4.1. Acquisition**

The acquisition of FBI-owned mobile devices must be made through procedures and processes established by the Procurement Section of FD.

Mobile devices must be listed on the FBI SPL prior to acquisition.

Procedures and processes regarding the acquisition of FBI-owned mobile devices intended for covert operations are described in the Undercover and Sensitive Operations Policy Guide, 0432PG.

**4.4.2. Section 508**

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794d), as amended, all mobile devices that the FBI develops, procures, maintains, or uses must provide disabled FBI personnel with equal or comparable access to, and use of, information and data as FBI personnel without disabilities. All requests for exemptions must be submitted to, and approved through, the [FBI Accessibility Program](#).

#### **4.4.3. Asset Management**

FBI-owned mobile devices are FBI property and must be accounted for and tracked in accordance with the procedures and processes established by the Asset Management Unit of FD.

Systems owners must establish criteria for FBI personnel to maintain FBI-owned mobile devices.

#### **4.4.4. Security Assessment and Authorization**

Systems owners must maintain security ATOs for USGI authorized to be processed, stored, or transmitted on FBI-owned mobile devices, in accordance with the requirements described in [Security Assessment and Authorization Policy Guide, 0655PG](#).

The use of FBI-owned mobile devices with non-FBI-owned IT devices and other FBI-owned IT devices must be documented in the SSP and approved by the FBI authorizing official.

Systems owners must assign personnel to document deviations from any requirements in this PG regarding FBI-owned mobile devices. Deviations must be approved by the FBI authorizing official and documented in the SSP.

#### **4.4.5. Marking**

FBI-owned mobile devices must be marked in accordance with the requirements described in [PD 0636D, External Security Marking of Information Technology Hardware and Electronic Data Storage Media](#).

#### **4.4.6. Configuration**

FBI-owned mobile devices must be configured in accordance with approved system security documentation pursuant to the [Security Assessment and Authorization Policy Guide, 0655PG](#).

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

#### 4.4.6.1. Data Containment

Systems owners must ensure USGI is restricted to FBI-approved secure container solutions or devices are running FBI-approved advanced monitoring tools at all times. Systems owners must also disable access to default e-mails, contacts, and calendar mobile apps (i.e., native apps) for the processing, storing, or transmission of USGI.

#### 4.4.7. Encryption

FBI-owned mobile devices must implement strong encryption for USGI at rest and in transit, in accordance with the requirements described in PD 0592D, *Encryption of Electronic FBI Information*.

##### 4.4.7.1. External Storage/Removable Media Encryption

Systems owners must assign personnel to encrypt all external storage/removable media for FBI-owned mobile devices.

#### 4.4.8. Malware Protection

FBI-owned mobile devices must employ malware protection to mitigate the risk of unauthorized access or disclosure of USGI.

#### 4.4.9. Service Management

Systems owners must establish procedures to review (at least monthly) voice and data usage and charges for FBI-owned mobile devices. This includes having procedures in place to identify voice and data under usage and over usage by FBI personnel on enterprise mobile devices.

A log must be maintained of FBI personnel with a history of over usage of enterprise mobile devices.

The MPO must review mobile service contracts for all enterprise devices at least quarterly, and must notify the FBI authorizing official if there are any significant over usage or under usage charges that cannot be promptly reconciled with the service provider.

##### 4.4.10. Mobile Application Management

Systems owners must establish a process to request, review, approve, update, and remove mobile apps for FBI-owned mobile devices.

All approved mobile apps must be added to the FBI's white list, and unapproved mobile apps must be added to the FBI's black list.

The FBI authorizing official (or designee) may release the mobile app to a limited group or groups of FBI personnel for testing purposes subsequent to the approval of a mobile app, but prior to its full release.

## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

#### 4.4.11. Mobile Infrastructure

The following are minimum requirements for the secure hosting, storage, management, control and/or transfer of USGI provided to or from mobile technologies.

FBI personnel designated as systems administrators of any cloud-based or mobile technologies must comply with the requirements described in PD 0875D, FBI Information Systems Privileged User Security Policy.

Systems owners must ensure that:

- Performance monitoring is conducted and security logs are maintained for a minimum of 90 calendar days, after which time the logs must be sent to the ESOC.
- Significant outages and down times of greater than 60 minutes are responded to within no more than two hours of receiving notification of the event.

Systems owners must define service-level agreements (SLA) and performance system recovery requirements in alignment with the availability requirements of the enterprise architecture objectives.

Information security requirements and standards for enterprise mobile technologies must be established and maintained by the MPO and SecD. Those procedures must contain the management of FBI-owned mobile device requirements described in this PG.

#### 4.4.12. Foreign Travel Device Configuration

Systems owners must ensure that all FBI-owned mobile devices taken on foreign travel have the applicable foreign travel baseline controls applied prior to traveling.

It is required that all FBI-owned mobile devices operating within high- or critical-threat countries be provided limited or no access to internal FBI networks and services.

##### 4.4.12.1. Foreign Travel Waivers

Systems owners must have a process in place for FBI personnel to request FBI-owned mobile devices be taken on foreign travel. See subsection 4.3.10 for procedures on the foreign travel process for enterprise mobile devices.

The FBI authorizing official must make an approval decision regarding the ability for FBI-owned mobile devices (other than laptops) to be taken on foreign travel to low- or moderate-threat countries, assuming all requirements identified in this PG are met.

The ESOC must also be notified of all foreign travel requests to low- or moderate-threat countries at least 48 hours prior to travel to allow for security monitoring of the device.



## UNCLASSIFIED

### Mobile Devices and Mobile Applications Policy Guide

DOJ IT Resources Outside of U.S. Territory Waiver Requests must be drafted and submitted to the FBI authorizing official for review for FBI-owned laptops to be taken on foreign travel to any country and FBI-owned mobile devices (other than laptops) to be taken on foreign travel to high- or critical-threat countries. Upon review, the FBI authorizing official must digitally sign the waiver and submit the request to the DOJ CISO for an approval decision. A DOJ IT Resources Outside of U.S. Territory Waiver Request will only be reviewed by the DOJ CISO for unclassified devices.

#### **4.4.12.2. Sensitive Data Storage**

Systems owners must reduce USGI on FBI-owned mobile devices. All documents, data, and mobile apps that are stored on a device and are not explicitly required for the trip must be removed.

#### **4.4.12.3. Two-Factor Tokens**

For travel to high- or critical-threat countries, systems owners are responsible for establishing current, two-factor authentication procedures (i.e., RSA SecurID tokens). If two-factor tokens have been issued, FBI personnel must keep hard tokens under positive control.

#### **4.4.13. Remote Administration**

The remote control of FBI-owned mobile devices may be authorized in the following circumstances:

1. When the location of FBI personnel is unknown or the location of an FBI device is unknown, the device may be remotely controlled by MPO or SecD in order to locate FBI personnel and/or to locate, recover, protect, or wipe USG equipment and data when authorized by the SC of the MPO or his or her designee. This includes the resetting of the password protecting any FBI-owned mobile device.
2. When FBI personnel are suspended, terminated, charged, or arrested for any type of misconduct or malfeasance, any FBI-owned devices within their possession or control may be remotely controlled by the MPO or SecD in order locate, recover, protect, or wipe USG equipment and data when authorization has been provided by the MPO SC, after consultation with OGC. This includes resetting passwords on any FBI-owned mobile device. When the FBI chooses to exercise this authority, the device, once remote control is initiated, must conspicuously alert the user and all present to the fact that the FBI is controlling the device through text on the screen, audible tone, and vibration, if available. This does not include authorization for the remote recording or capture of sound or images. Remote control for investigative purposes must be coordinated with, and approved by, the OGC and/or DOJ.

FBI personnel who are issued FBI-owned mobile devices must be provided written notification in advance of these provisions.

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

**4.4.14. Collection of Data Analytics**

Systems owners and SecD are authorized to collect generalized information regarding usage, user location, and other service trends for performing data analytics. Information collected for performing data analytics must not contain or transmit PII without the approval of OGC.

**4.4.15. Sanitization and Destruction**

Sanitization and destruction of FBI-owned mobile devices and associated mobile infrastructure must be performed in accordance with the requirements described in PD 0506D, *Destruction of Classified and Sensitive Material*.

Systems owners must establish a process for sanitizing and destroying FBI-owned mobile devices and associated mobile infrastructure. This process must be approved by the FBI authorizing official, in accordance with the *Security Assessment and Authorization Policy Guide, 0655PG*.

**4.5. Exemptions and Exceptions**

Exemptions to the security procedures and processes must be documented in the SSP for FBI-owned mobile devices. Approvals are granted through the SAA process, as described in PD 0655D, *Security Assessment and Authorization for FBI Information Systems*.

Exemptions to the MPO process and procedures in this PG must be approved by the FBI authorizing official (or designee) and documented in the MPO's Sentinel case file

The FBI authorizing official may only designate authority for exemption approvals to persons holding Senior Executive Service (SES) or Senior Level (SL) positions or higher.

b7E

Individual exceptions to the procedures and processes within this PG must be approved by the responsible AD. To determine who the responsible AD is, refer to the roles and responsibilities section of this PG (Section 2) or consult with the Internal Policy Office (IPO) of the Resource Planning Office (RPO).

UNCLASSIFIED

Mobile Devices and Mobile Applications Policy Guide

## 5. Summary of Legal Authorities

---

### 5.1. Federal

- National Security Act of 1947, as amended
- The Rehabilitation Act of 1973, as amended Title 29 United States Code (U.S.C.) Section (§) 794d
- Intelligence Reform and Terrorism Prevention Act of 2004
- Federal Information Security Modernization Act (FISMA) of 2014
- Clinger-Cohen Act of 1996, repealed and reenacted as 40 U.S.C. § 11101, et seq.
- [EO 13526, Classified National Security Information](#)
- [EO 13589, Promoting Efficient Spending](#)

### 5.2. Intelligence Community Directives (ICD)

- [ICD Number 705, Sensitive Compartmented Information Facilities](#)

### 5.3. Committee on National Security Systems (CNSS)

- [CNSSAM TEMPEST/01-13, RED/BLACK Installation Guidance](#) (links to a U//~~FOUO~~ document)
- [Committee on National Security Systems Policy \(CNSSP\) No. 17, Policy on Wireless Systems](#)

### 5.4. Department of Justice

- [DOJ Order 0901, Insider Threat](#)
- [DOJ Order 2640.2F, Information Technology Security](#)
- [DOJ Order 2740.1A, Use and Monitoring of DOJ Computers and Computer Systems](#)
- [DOJ Order 2880.1C, Information Resource Management Program](#)
- DOJ Order 0902, Accessible Electronic and Information Technology, 10/15/2015

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

**6. Recordkeeping Requirements**

---

Records associated with, or created on, FBI-owned mobile devices must be maintained by FBI personnel in accordance with the *Records Management Policy Guide, 0769PG*, under appropriate case file numbers and stored in an FBI information system that maintains official records in accordance with the *Electronic Recordkeeping Certification Policy Guide, 0800PG*.

When using mobile apps on FBI-owned mobile devices for operational purposes, systems owners must ensure that all records are uploaded to appropriate FBI case files as soon as practicable after creation. Since there is a potential for creating federal records, systems owners must ensure that FBI personnel can export any captured information into an FBI recordkeeping system prior to implementation.

UNCLASSIFIED

Mobile Devices and Mobile Applications Policy Guide

**Appendix A: Final Approvals**

MOBILE DEVICE AND MOBILE APPLICATION POLICY GUIDE	
<b>Date of Last Review</b>	None
<b>Publish Date</b>	2016-07-06
<b>Effective Date</b>	2016-07-06
<b>Review Date</b>	2017-07-06
EXEMPTIONS	
1. Mobile devices containing digital evidence are exempt from this PG. Refer to the <i>Digital Evidence Policy Directive and Policy Guide, 0639DPG</i> , for more information.	
2. FBI-owned mobile devices described as technical or scientific products (TSP) are exempt from this PG. Refer to <i>PD 0378D, Technical or Scientific Products Procurement Policy Directive</i> for more information.	
3. FBI-owned mobile devices acquired for nonoperational use such as testing or investigative training are exempt from the acquisition requirements of this PG but must meet all other asset management requirements for accountability and tracking of FBI property.	
4. Mobile devices owned by emergency medical technicians (EMT) are exempt from this PG.	
5. Court-ordered personal monitoring devices are exempt from this PG.	
REFERENCES	
1. <i>Attachment A, Mobile Device Restrictions Quick Reference Guide (ORG)</i>	
2. <i>Attachment B, Laptops in FBI Sensitive Compartmented Information Facilities Quick Reference Guide (ORG)</i>	
3. <i>Classification 319, Managing the FBI's Administrative Records</i>	
4. Committee on National Security Systems Instruction (CNSSI) No. 22, <i>Policy on Information Assurance Risk Management for National Security Systems</i>	

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

5. <u>CNSSI No. 4009, <i>National Information Assurance (IA) Glossary</i></u>
6. <u>FD-1001, "Consent for Warrantless Searches of Department of Justice Workplaces"</u>
7. <u><i>Courier Program Policy Directive and Policy Guide, 0719DPG</i></u>
8. <u><i>Digital Evidence Policy Directive and Policy Guide, 0639DPG</i></u>
9. <u>DOJ Mobile Device and Mobile Application Security Policy Instruction</u>
10. <u>EO10096, <i>Providing for a Uniform Patent Policy for the Government with respect to Inventions made by Government Employees and for the Administration of Such Policy</i></u>
11. <u>EO 13556, <i>Controlled Unclassified Information</i></u>
12. <u>FBI Critical and High Threat Country Life Safety List</u>
13. <u><i>FBI Ethics and Integrity Program Policy Directive and Policy Guide, 0754DPG</i></u>
14. <u><i>FBI Memoranda of Understanding and Non-Contractual Agreements Policy Implementation Guide, 0273PG</i></u>
15. <u>FBI SPL</u>
16. <u><i>Frequently Asked Questions Regarding Social Media and the Hatch Act</i></u>
17. <u><i>Government Vehicle Use Policy Guide, 0791PG</i></u>
18. <u>ICD Number 503, <i>Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation</i></u>
19. <u>ICD Number 705, <i>Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities</i></u>
20. <u>Information and Technology Branch (ITB) Enterprise Mobility Strategy</u>
21. <u>Information Assurance (IA) Policy Compliance Assessment Plan</u>
22. <u>Instructions for DOJ IT Resources Outside of U.S. Territory Waiver Request</u>
23. <u>National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision (Rev.) 1, <i>Guide for Conducting Risk Assessments</i></u>

UNCLASSIFIED

Mobile Devices and Mobile Applications Policy Guide

24. <u>NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems</u>
25. <u>PD 0247D, Removable Electronic Storage (RES) Media Protection</u>
26. <u>PD 0329D, Official Foreign Travel</u>
27. <u>PD 0378D, Technical and Scientific Products Procurement Policy Directive</u>
28. <u>PD 0380D, Unofficial Foreign Travel</u>
29. <u>PD 0506D, Destruction of Classified and Sensitive Material</u>
30. <u>PD 0592, Encryption of Electronic FBI Information</u>
31. <u>Security Compliance Program PG. 0934PG</u>
32. <u>PD 0636D, External Security Marking of Information Technology Hardware and Electronic Data Storage Media</u>
33. <u>PD 0655D, Security Assessment and Authorization for FBI Information Systems</u>
34. <u>PD 0723D, Federal Bureau of Investigation (FBI) Unclassified Network (UNet) Enclave Policy</u>
35. <u>PD 0727D, Non-Retaliation for Reporting Compliance Risks</u>
36. <u>PD 0796D, Reporting FBI Employee Misconduct</u>
37. <u>PD 0919D, FBI Accessible Information and Communication Technology Policy</u>
38. Presidential and Federal Records Act Amendments of 2014
39. <u>FD-281, "Receipt for Government Property"</u>
40. <u>Records Management Policy Guide, 0769PG</u>
41. Rehabilitation Act of 1973
42. <u>Remote Access for General and Privileged Users Policy Guide, 0655PG-4</u>

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

43. <u>Safeguarding Classified National Security Information Directive and Policy Implementation Guide, 0632PG</u>	
44. <u>Section 508 Program Team</u>	
45. <u>Security Assessment and Authorization Policy Guide, 0655PG</u>	
46. <u>Social Media and Other Electronic Information Sharing Technologies Policy Directive and Policy Guide, 0579DPG</u>	
47. <u>Undercover and Sensitive Operations Policy Guide, 0432PG</u>	
<b>APPROVALS</b>	
<b>Sponsoring Executive Approval</b>	<b>Clifford C. Holly</b> Assistant Director Security Division
<b>Sponsoring Executive Approval</b>	<b>Jon K. Reid</b> Acting Assistant Director Information Technology Infrastructure Division
<b>Executive Assistant Director Approval</b>	<b>Valerie Parlave</b> Executive Assistant Director Human Resources Branch
<b>Final Approval</b>	<b>James L. Turgal</b> Executive Assistant Director Information Technology Branch



**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

**Appendix B: Sources of Additional Information**

---

<b>Information Assurance Section, Security Division</b>
<u>Assurance Management Unit</u>
<b>Collaboration and Compliance Section, Information Technology Infrastructure Division</b>
<u>Mobility Program Office</u>

UNCLASSIFIED

Mobile Devices and Mobile Applications Policy Guide

**Appendix C: Contact Information**

<b>Security Division</b>	
Information Assurance Section	
Assurance Management Unit	J. Edgar Hoover Building 935 Pennsylvania Avenue, NW Washington, DC 20535
Security Division Policy Officer	

b6  
b7C  
b7E

<b>Information Technology Infrastructure Division</b>	
Collaboration and Compliance Section	
Mobility Program Office	J. Edgar Hoover Building 935 Pennsylvania Avenue, NW Washington, DC 20535
Mobility Program Office Supervisor	

UNCLASSIFIED

Mobile Devices and Mobile Applications Policy Guide

**Appendix D: Definitions and Acronyms**

---

**Definitions:**

<b>Application program interface</b>	A set of routines, protocols, and tools for building software applications. An API expresses a software component in terms of its operations, inputs, outputs, and underlying types.
<b>Authorizing official</b>	An entity with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [Source: Derived from <u>CNSSI No. 4009, National Information Assurance (IA) Glossary</u> ]
<b>Black list</b>	A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity. [Source: <u>CNSSI No. 4009, National Information Assurance (IA) Glossary</u> ]
<b>Bring your own device</b>	The practice of employers or organizations allowing personnel to use personally owned mobile devices for official business, often permitting access to privileged or otherwise sensitive data or systems.
<b>Cloud resource</b>	A type of computing that relies on sharing resources rather than having local services, servers, or personal devices to handle computing workloads. There are two types of cloud-based resources: <ol style="list-style-type: none"><li>1. Infrastructure as a Service (IaaS) refers to on-demand, data-center-like infrastructure offered by a third party with pay-as-you-go pricing. Clients may create and deliver services and applications to customers leveraging just-in-time compute resources from either physical or virtual machines provided by the third party. IaaS cloud compute resources generally consist of storage, database (including relational and not only structured query language [NoSQL]), compute memory and may include other capabilities such as data backup, management tools, and network services (including software-defined networks).</li><li>2. Software as a Service (SaaS) or Platform as a Service (PaaS) are cloud-based resources provided by a third party that offer additional value-added services or capabilities beyond that provided at the IaaS level. Capabilities are generally provided based on a subscription model that may include propriety or open-source software.</li></ol>
<b>Cloud service</b>	A model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable Internet accessible cloud resources.

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

<b>Covert operation</b>	See <u>undercover operation</u> .
<b>Enterprise mobile device</b>	An FBI-owned mobile device issued by the MPO that is associated with an enclave FBI information system.
<b>FBI information system</b>	A set of FBI information resources organized for the acquisition, collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. [Source: Derived from <u>CNSSI No. 4009, National Information Assurance (IA) Glossary</u> ]
<b>FBI personnel</b>	Any individual employed by, detailed to, or assigned to the FBI, including interns; joint task force members; members of the armed forces; expert consultants to the FBI; industrial or commercial contractors, licensees, certificate holders, or grantees of the FBI, including all subcontractors or personal service contractors of the FBI; or any other person who acts for or on behalf of the FBI, as determined by the FBI Director.
<b>FBI-controlled facility</b>	A temporary or permanent area where the FBI exercises authority and control. This includes office work space, conference rooms, cafeteria areas, break rooms, and hallways connecting these spaces.
<b>IT Resource</b>	Any information system, device, network, or account that processes, stores, or transmits information.
<b>Logical connection</b>	Connection of a device to an information system, another device, a network, or an account through a server or network configuration.
<b>Logical HTTPS</b>	HTTPS, also called HTTP over Transport Layer Security (TLS) or HTTP over Secure Socket Layer (SSL). Logical HTTPS provides authentication and encrypted communications, increasing trust that the Web server or API is the intended recipient of the request. Logical HTTPS or Web-moderated communication channels provide limited, controlled, secured, and auditable interactions over the Internet. Conversely, lower-level connections such as wired, Bluetooth, direct Wi-Fi, and NFC, within the Open System Interconnection (OSI) Model, may grant more wide-ranging authorities, have fewer audit controls, and must rely on network-based packet capture and/or deep packet inspection in order to audit user interactions.
<b>Medical device</b>	A device prescribed for the purposes of maintaining life standards (e.g., hearing aids, pacemakers, implanted medical devices).
<b>Mobile application</b>	A mobile application, or “mobile app,” is application software designed to run on a mobile device to provide users with services similar to those accessed on desktop computers.

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

<b>Mobile backend</b>	The suite of features including cloud services, platform services, and software utilities required by mobile devices and mobile applications to function. It enables a range of common controls such as security, data management, authentication, and storage.
<b>Mobile device</b>	<p>A portable computing device that:</p> <ul style="list-style-type: none"> <li>• Is physically small and can easily be carried by a single individual.</li> <li>• Is designed to operate without a physical connection (e.g., wirelessly transmit or receive information).</li> <li>• Possesses local, nonremovable data storage.</li> <li>• Is powered-on for extended periods of time with a self-contained power source.</li> </ul> <p>Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. [Source: Derived from <u>CNSSI No. 4009, National Information Assurance (IA) Glossary</u>]</p>
<b>Mobile infrastructure</b>	<p>The mobile infrastructure is a comprehensive hosting environment for enterprise mobile services that provides the following functions:</p> <ul style="list-style-type: none"> <li>• The MDM or a successor service</li> <li>• The MAM or a successor service</li> <li>• The mBaaS API or a successor service</li> <li>• Computing, storage, and analytics enabling content provided to end-user devices</li> </ul>
<b>Near-field communication</b>	A set of standards for mobile devices to establish radio communication with each other by touching them together or bringing them into close proximity.
<b>Non-FBI-owned mobile device</b>	A mobile device that is OGA (including local, state, and tribal law enforcement)-, contractor-, vendor-, or visitor-owned or is personally owned.
<b>OGA-owned mobile device</b>	A government-furnished or local, state, or tribal law enforcement device issued for the purposes of official USG business.
<b>Overt operation</b>	FBI missions and functions that occur on a normal day-to-day basis.
<b>Personally identifiable</b>	PII has been defined by the Office of Management and Budget (OMB) as information that can be used to distinguish or trace an individual’s identity, such as name, social security number, or biometric records, alone or when

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

<b>information</b>	combined with other personal or identifying information that is linked or linkable to a specific individual, such as date or place of birth or mother's maiden name.
<b>Product charter</b>	A formal statement of goals and objectives that defines a business problem, establishes a plan for addressing the problem—and once approved—authorizes the work to execute the plan.
<b>Proxy</b>	An intermediary resource in the form of a computer system or an application that acts as a third party for requests and responses between two clients.
<b>Reasonable suspicion</b>	An objectively justifiable suspicion that is based on specific facts or circumstances that justifies stopping and sometimes searching a person thought to be involved in criminal activity at the time.
<b>Record</b>	All recorded information, regardless of form or characteristics, made or received by a federal agency under federal law, or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the USG or because of the informational value of data in them. Records do not include library or museum materials made or acquired and preserved solely for reference or exhibition purposes or duplicate copies of records preserved for convenience. Recorded information includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.
<b>Red/black separation</b>	Separation of electrical and electronic circuits, components, equipment, and systems that handle unencrypted information (red), in electrical form from those that handle encrypted information (black) in the same form. [Source: Derived from <u>CNSSI No. 4009, <i>National Information Assurance (IA) Glossary</i></u> ]
<b>Remote desktop protocol</b>	Software or operation system features allowing an individual to access a computer desktop or server resource remotely from a local client system such as a personal computer. In general, the term is used here where little or no information is stored locally on the local machine once a session is terminated.
<b>Resource</b>	A source or supply from which benefit is produced. Typically, resources are materials, energy, services, staff, knowledge, or other assets.
<b>Security</b>	The practice of monitoring, tracking, logging, analyzing, and responding,

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

<b>monitoring</b>	often in real-time, with the controls or mitigations for information system or user activities necessary to ensure the confidentiality, integrity, and availability of resources and data.
<b>Sensitive Compartmented Information facility</b>	Accredited area, room, or group of rooms, buildings, or installation where sensitive compartmented information may be stored, used, discussed, and/or processed. [Source: <u>CNSSI No. 4009, <i>National Information Assurance (IA) Glossary</i></u> ]
<b>Signal enhancement device</b>	A device that takes an existing signal from an access point or wireless router and rebroadcasts it to create a second network.
<b>Stand-alone device</b>	A computer resource that is not directly connected to a corporate network, but may be connected to the Internet.
<b>Strong encryption</b>	An encryption algorithm that is generally more resistant to attack than other encryption algorithms. Currently, the accepted level of strong encryption is defined by TLS 1.2 or IPSECURITY leveraging Advanced Encryption Standard (AES) 256 or similar encryption standards.
<b>System security documentation</b>	Formal documentation prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The documentation can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. [Source: Derived from <u>CNSSI No. 4009, <i>National Information Assurance (IA) Glossary</i></u> ]

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

<p align="center"><b>Technical or scientific product</b></p>	<p>IT equipment, supplies, and services that are not connected to any FBI enterprise network, and are used to:</p> <p>(1) Intercept, capture, collect, or record audio, video, image, or digital data in the course of surveillance activities;</p> <p>(2) Exploit secure technologies or protect covert operations; or</p> <p>(3) Conduct scientific research, laboratory, or forensic analysis. Examples include workstations, laptops, peripherals, servers, routers, encryption devices, digital storage devices and media, telecommunications equipment, and software used to intercept, map/locate, collect, process, transmit, route, or temporarily store raw surveillance data, defeat secure technologies, defend covert operations, conduct scientific research, or perform forensic analysis of digital or physical evidence. Also included are services used to acquire, develop, or maintain systems and assets related to scientific, laboratory, or forensic research and analysis, secure technologies, communications intercept, and covert operations. [Source: <u>PD 0378D, Technical and Scientific Products Procurement Policy Directive</u>]</p>
<p align="center"><b>TEMPEST</b></p>	<p>A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. [Source: <u>CNSSI No. 4009, National Information Assurance (IA) Glossary</u>]</p>
<p align="center"><b>Undercover operation</b></p>	<p>FBI missions and functions that include Group I, Group II, or <input type="text"/> undercover or sensitive operations.</p>
<p align="center"><b>United States government information</b></p>	<p>Information that either (1) meets the standards for national security classification under EO 13526, as amended, or (2) is unclassified information that does not meet the standards for national security classification under EO 13526, as amended, but is (a) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (b) under law or policy requires protection from unauthorized disclosure. [Source: Derived from <u>CNSSI No. 4009, National Information Assurance (IA) Glossary</u>]</p>
<p align="center"><b>Virtual Private Network</b></p>	<p>Extends a private network across a public network such as the Internet. It enables clients to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus are benefiting from the functionality, security, and management resources of the private network. However, it also increases the risk of unauthorized and unwanted malware transfer to gain access to a private network.</p>
<p align="center"><b>Wearable</b></p>	<p>Electronics that may be integrated into clothing or accessories, incorporating simple compute and or advanced electronic capabilities. Items such as activity trackers, smart watches, and other sensor-type devices are</p>

b7E



**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

	generally categorized as an Internet of Things (IoT). Examples include wearable technology, wearable devices, and smart wearable devices.
<b>White list</b>	A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system. [Source: <a href="#"><u>CNSSI No. 4009, National Information Assurance (IA) Glossary</u></a> ]
<b>Wireless connection</b>	Connection of a device to a separate information system, device, network, or other resource through wireless technology (e.g., Wi-Fi, Bluetooth, or NFC).

**Acronyms:**

AD	assistant director
ADA	Americans with Disabilities Act
AES	Advanced Encryption Standard
API	application program interface
App	application
ARU	Accounts Receivable Unit
AS	Accounting Section
ASAC	assistant special agent in charge
ATO	Authorization to Operate
BRMS	Business Relationship Management Section
BYOD	bring your own device
CART	Computer Analysis Response Team
CCS	Collaboration and Compliance Section
CD	compact disc
CDC	chief division counsel
CFR	Code of Federal Regulations

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

CIO	chief information officer
CISO	chief information security officer
CMDU	Creative Media Development Unit
CMS	Curriculum Management Section
CNSS	Committee on National Security Systems
CNSSAM	Committee on National Security Systems Advisory Memorandum
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COOP	continuity of operations
CSMU	Career Services Management Unit
CSO	chief security officer
DFAS	Digital Forensics and Analysis Section
DIOG	<i>Domestic Investigations and Operations Guide</i>
DOJ	Department of Justice
DPO	division policy officer
DVD	digital versatile disc
EAD	executive assistant director
EC	electronic communication
EMT	emergency medical technician
EO	executive order
ERC-WG	enterprise requirements and capabilities working group
ERKC	electronic recordkeeping certification
ESOC	Enterprise Security Operations Center
FBI	Federal Bureau of Investigation

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

FD	Finance Division
FISMA	Federal Information Systems Modernization Act
FO	field office
<del>FOUO</del>	<del>For Official Use Only</del>
GPS	Global Positioning System
HIPPA	Health Insurance Portability and Accountability Act
HTTPS	Secure Hypertext Transfer Protocol
IA	information assurance
IaaS	Infrastructure as a Service
IAS	Information Assurance Section
IATU	Information Assurance Technology Unit
IC	Intelligence Community
ICD	Intelligence Community Directive
IIS	Internal Investigations Section
INSD	Inspection Division
InTC	Insider Threat Center
IPO	Internal Policy Office
IoT	Internet of Things
ISA	interconnection security agreement
ISP	Internet service provider
IT	information technology
ITB	Information Technology Branch
ITCRMD	Information Technology Customer Relationship and Management Division

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

ITID	Information Technology Infrastructure Division
ITP&M	information technology portfolio manager
ITS	information technology specialist
JMD	Justice Management Division
LES	Law Enforcement Sensitive
MAM	mobile application management
mBaaS	mobile backend as a service
MDM	mobile device management
MMS	Multimedia Messaging Service
MOA	memorandum of agreement
MOU	memorandum of understanding
MPO	Mobility Program Office
MSS	Mission Support Section
MST	mobile surveillance team
MTN	mobile telephone number
NFC	near-field communication
NIST	National Institute of Standards and Technology
NoSQL	Not only Structured Query Language
OCONUS	outside the continental United States
OGA	other government agency
OGC	Office of the General Counsel
OMB	Office of Management and Budget
OSI	open system interconnection
OTA	over-the-air

**UNCLASSIFIED**

Mobile Devices and Mobile Applications Policy Guide

OTD	Operational Technology Division
OWA	Outlook Web Application
PaaS	Platform as a Service
PAU	Product Assurance Unit
PD	policy directive
PG	policy guide
PII	personally identifiable information
POC	point of contact
PSU	Physical Security Unit
QRG	quick reference guide
RDP	Remote Desktop Protocol
RES	removable electronic storage
Rev.	revision
RPO	Resource Planning Office
SAA	security assessment and authorization
SaaS	Software as a Service
SC	section chief
SCIF	Sensitive Compartmented Information facility
SecD	Security Division
SES	Senior Executive Service
SIM	subscriber identification module
SL	Senior Level
SLA	service level agreement
SMS	Short Messaging Service

**UNCLASSIFIED**

## Mobile Devices and Mobile Applications Policy Guide

SOS	Security Operations Section
SP	special publication
SPL	Standard Products List
SSL	Secure Socket Layer
SSP	system security plan
TCSU	Training Coordination and Support Unit
TD	Training Division
TDY	temporary duty [assignment]
TLS	Transport Layer Security
TODU	Technically Trained Agent Operations and Development Unit
ToU	terms of agreement
TPS	Technical Programs Section
TSP	technical or scientific product
UC	unit chief
UNet	Unclassified Network
USB	Universal Serial Bus
U.S.C.	United States Code
USG	United States government
USGI	United States government information
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network
Wi-Fi	wireless fidelity
WPA2	Wi-Fi Protected Access II

UNCLASSIFIED

Mobile Devices and Mobile Applications Policy Guide

**Appendix E: Security Controls Policy Reference Matrix**

---

The Security Controls Policy Reference Matrix identifies the required security controls regarding mobile devices and the associated policy references in this PG.

An "X" or a "+" indicates that the security control is required for the system in accordance with the *Security Controls for FBI Information Systems*.

Security Control	Policy Reference in this PG	Confidentiality			Integrity			Availability		
		Low	Mod.	High	Low	Mod.	High	Low	Mod.	High
AC-19	3.2, 3.3.2	X	X	X	X	X	X			
AC-19 (5)	3.2		X	X		X	X			

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION  
**POLICY DIRECTIVE**

**0353D**

<b>1. Policy Directive Title.</b>	(U) Software Assurance Security Policy
<b>2. Publication Date.</b>	2011-07-27
<b>3. Effective Date.</b>	2011-07-27
<b>4. Review Date.</b>	2020-11-01
<b>5. Date of Last Renewal</b>	9/21/2017

**6. Authorities:**

- 6.1. (U) National Security Act of 1947, as amended
- 6.2. (U) Clinger-Cohen Act, repealed and reenacted as Title 40 United States Code (U.S.C.) Section (§) 11101 *et seq.*
- 6.3. (U) Department of Justice (DOJ) 2640.2F, Information Technology Security, November 26, 2008
- 6.4. (U) Director of Central Intelligence Directive (DCID) 7/6. Community Acquisition Risk Center, March 2, 2005
- 6.5. (U) OMB Memorandum M-04-16, Software Acquisition, July 1, 2004
- 6.6. (U) OMB Memorandum M-04-08, Maximizing Use of SmartBuy and Avoiding Duplication of Agency Activities with the Presidents 24 E-Gov Initiatives, April 2004
- 6.7. (U) OMB Memorandum M-05-23, Memorandum for Chief Information Officers, Improving Information Technology (IT) Project Planning and Execution, August 4, 2005

**7. Purpose:**

- 7.1. (U) This policy establishes security assurance requirements for software used by the Federal Bureau of Investigation (FBI).
- 7.2. (U) Software Provenance. This policy requires implementation of specific methods to assure that software is acquired by the FBI from reliable sources, and is adequately protected throughout its useful life cycle.
- 7.2.1. (U) Software is a malleable asset that can be used or misused to damage the FBI through sabotage or subversion at any point within the software supply chain.
- 7.2.2. (U) Software may contain tangible indications of sensitive information, sources, methods, operations, identities, techniques, standards, technologies, plans, records, and procedures used by the FBI in conducting its mission.
- 7.2.3. (U) Software may contain exploitable vulnerabilities that can be used to subvert, sabotage, intercept, or disclose sensitive FBI information.
- 7.3. (U) Life Cycle Integration. Software assurance requires integration of security review and assessment with life cycle management processes as described in the FBI Information Technology (IT) Life Cycle Management (LCM) Handbook, FBI Electronic Record Keeping Certification (ERKC) Manual, and the FBI Certification and Accreditation (C&A) Handbook.
- 7.4. (U) Software Security Assurance Implementation Procedures. This policy directive uses existing LCM processes, Electronic Records Management (ERM) processes, Information Assurance C&A processes, and Software Acquisition processes as defined in the FBI IT LCM Handbook, the EKRC Manual, the FBI C&A Handbook, and Finance and Security acquisition processes as implementation guidance for this policy directive.

**8. Policy Statement:**

- 8.1. (U) Software Use. The FBI must use software only in compliance with provisions of software licenses, applicable statutes and orders, and Information System (IS) security authorizations.
- 8.2. (U) Software Assurance. The FBI must acquire, protect, maintain, control, and manage software in compliance with Federal laws and directives, and in compliance with FBI IT LCM Handbook, and the FBI C&A Handbook.
- 8.2.1. (U) Software Acquisition.
- 8.2.1.1. (U) The FBI must use software that is acquired through approved FBI acquisition processes.
- 8.2.1.2. (U) To the extent possible, the FBI must acquire software compliant with security criteria established by the Assistant Director (AD) for Security Division.
- 8.2.2. (U) Software Protection. The FBI must protect software from unauthorized access and modification as defined in the FBI IT LCM Handbook and the FBI C&A Handbook.
- 8.2.3. (U) Software Maintenance. The FBI must maintain the currentness of security relevant software, including versions, patches, upgrades, updates, and implementation of countermeasures according to the FBI Vulnerability Patch Management Policy Directive (OXTBD).
- 8.2.4. (U) Software Control.
- 8.2.4.1. (U) Change Control. The FBI must ensure that all authorized software changes are compliant with the FBI IT LCM Handbook.
- 8.2.4.2. (U) Version Control. The FBI must implement procedures for software version tracking and control compliant with the FBI IT LCM Handbook.
- 8.2.5. (U) Software Management. The FBI must manage software through configuration management processes as described in the FBI IT LCM Handbook.
- 8.2.6. (U) Software Removal. Software that is no longer authorized must be removed from FBI systems.



8.2.7. (U) Security Issues. To the extent practicable, known and newly discovered security issues surrounding software used at the FBI must be reported to the Enterprise Security Operations Center (ESOC) through the Security Incident Reporting System (SIRS).

8.2.8. (U) Software Provenance. Software acquisition decisions must address, as far as practical, the source and provenance of software products including foreign influence exerted over software developers, vendors, and suppliers.

8.2.8.1. (U) Open Source Software (OSS). The FBI must use OSS on FBI operational systems only after that software has been evaluated by the acquiring program/project manager or cognizant supervisor.

8.2.8.1.1. (U) Evaluations may incorporate information from internal FBI sources and from competent external authorities such as the National Information Assurance Partnership (NIAP), the National Institutes of Standards and Technology (NIST), and other government agencies (OGA) that are chartered to perform security evaluations.

8.2.8.1.2. (U) The Office of General Counsel (OGC) must review licensing provisions of OSS as an element of evaluation, as appropriate.

8.2.8.2. (U) Software from sources that are under Foreign Ownership, Control, or Influence (FOCI) Software. FOCI software may not be used on FBI Critical Assets that process National Security Information unless approved by the AD for Security Division and the FBI authorizing official.

8.2.8.2.1. (U) The AD for Security Division may require an Acquisition Risk Directorate (ARD).

8.2.8.3. (U) Software of Unknown Pedigree (SOUP). Software packages that do not have an identifiable, trustworthy source must not be acquired, installed, or used on FBI operational systems without approval of the AD for Security Division, the FBI CIO, the OGC, the Finance Division (FD) Procurement Section, and the appropriate Head of Division or their designee(s).

8.3. (U) Software in Evaluation and Development Environments. Commercial off the shelf software (COTS), Government off the shelf software (GOTS), OSS, and SOUP that is acquired through FBI approved acquisition processes may be used for FBI evaluation, for FBI development activities, and for component monitoring activities that are separated from the FBI operational systems and networks and from FBI sensitive information with approval of the development or evaluation program/project manager or cognizant supervisor.

8.3.1. (U) Software that is used in evaluation or development environments may not be introduced into FBI operational systems without approval according to sections 8.1 and 8.2 of this policy.

8.4. (U) Legal Rights. Regardless of any contract language, licensing provision, or other agreement, the FBI reserves the legal right and is obligated to impose any legal security methods, safeguards, and restrictions deemed necessary to ensure:

8.4.1. (U) Unauthorized access to National Security Information or Law Enforcement Information is effectively precluded.

8.4.2. (U) The ability of the FBI to perform its mission or to protect United States Government Protected Information (USGPI) is not adversely affected by complying with provisions of the software license.

8.5. (U) Unauthorized Software.

8.5.1. (U) Introduction of any unauthorized software into any FBI IS may be justification for administrative, criminal, or other adverse disciplinary action.

8.5.2. (U) Introduction of unauthorized software into any FBI IS may be justification for review of the Approval to Operate (ATO) for that IS according to the Security Assessment and Authorization for FBI Information Systems Policy Directive (0655D).

## 9. Scope:

9.1. (U) The Software Security Assurance Policy applies to all Software acquired for and used on FBI owned and operated systems.

9.2. (U) Software Categories. For the purposes of this policy directive, software, including software that is embedded in hardware devices, is categorized into the following overlapping types:

- Standard commercial and U.S. Government developed software.
- Open Source Software (OSS).
- Software developed or managed under Foreign Ownership, Control, or Influence (FOCI Software).
- Software of Unknown Pedigree (SOUP).

9.3. (U) This policy directive does not supersede any existing acquisition policy directives or procedures of the FBI.

## 10. Proponent:

(U) Security Division

(U) Information Assurance Section

## 11. Roles and Responsibilities:

11.1. (U) Assistant Director for Security Division must:

11.1.1. (U) Investigate violations of this policy and enforce sanctions when appropriate.

11.1.2. (U) Ensure that security equities are represented on Life Cycle Management (LCM) boards and within LCM processes.

11.1.3. (U) In conjunction with the Executive Assistant Director, Information and Technology Branch (EAD-ITB), Executive Assistant Director, Science and Technology Branch (EAD-STB), and FD, establish business practices to oversee acquisition of FOCI software for FBI critical information system and technical system assets.

11.1.4. (U) Serve as the FBI referent for the Acquisition Risk Directorate (ARD) of the National Counterintelligence Executive for the Director of National Intelligence, to collect and disseminate counterintelligence and security information concerning companies, software, and countries of concern, as appropriate.

11.1.5. (U) With the FBI Chief Information Officer (CIO) for IS, or the EAD-STB for technical systems, as appropriate, ensure mitigation of known, and newly discovered, security risks for FBI software.

- 11.1.6. (U) Make approval recommendations for exemptions to this policy in conjunction with the FBI CIO for IS or the EAD-STB for technical systems, as appropriate.
- 11.1.7. (U) Establish business practices, procedures, or mechanisms to share appropriate software security assurance information, including evaluations, across the U.S. Government, Department of Justice (DOJ), and the FBI.
- 11.1.8. (U) Establish security evaluation criteria for acquisition of software that is to be used on FBI operational systems.
- 11.1.9. (U) With the FBI Authorizing Official and FD, establish business practices to oversee the acquisition of software for use on FBI critical assets.
- 11.1.10. (U) Ensure that FBI contracts contain software assurance language according to this policy directive.
- 11.2. (U) Executive Assistant Director, Information and Technology Branch, Chief Information Officer must:
- 11.2.1. (U) Include software security assurance standards and security representation in FBI Life Cycle Management Directives and IT governance Processes.
- 11.2.2. (U) Make approval decisions for exemptions to this policy in conjunction with the AD for Security Division, as appropriate.
- 11.2.3. (U) With the AD for Security Division and the FD, establish business practices to oversee acquisition of software for FBI critical IS assets.
- 11.3. (U) Executive Assistant Director, Science and Technology Branch must:
- 11.3.1. (U) Include software security assurance standards and security representation in FBI LCM directives and IT Governance Processes.
- 11.3.2. (U) Make approval decisions for exemptions to this policy in conjunction with the AD for Security Division, as appropriate.
- 11.3.3. (U) With the AD for Security Division and the FD, establish business practices to oversee acquisition of software for FBI critical technical system assets that include software security assurance standards.
- 11.4. (U) The Assistant Director for Finance Division must:
- 11.4.1. (U) In conjunction with the AD for Security Division, establish business practices to oversee acquisition and procurement of software for the FBI that include software security assurance standards.
- 11.5. (U) Information System Security Manager (ISSM) must:
- 11.5.1. (U) Ensure implementation of this policy for IS under their cognizance.
- 11.5.2. (U) Report violations of this policy through the SIRS.
- 11.5.3. (U) With the Information System Owner and the System Administrator, review software holdings and develop plans for elimination of unauthorized software.
- 11.5.4. (U) With the Information System Owner and the System Administrator, ensure that new software to be added to an FBI IS is evaluated for compatibility with existing software.
- 11.6. (U) Office of General Counsel must:
- 11.6.1. (U) Advise FBI components concerning the legal ramifications, obligations, and prohibitions contained in software licenses.
- 11.6.2. (U) Advise FBI components concerning legal licensing restrictions, rights, and obligations in the use of software.
- 11.6.3. (U) Advise the AD for Security Division, the FBI CIO, Heads of Divisions, and program/project managers on legal issues of concern with acquisition and use of OSS and SOUP on FBI systems.
- 11.6.4. (U) Advise the AD for Security Division on legal issues regarding software assurance contract language.
- 11.7. (U) Heads of Divisions as Information System Owners must:
- 11.7.1. (U) Ensure that Division users comply with this policy.
- 11.7.2. (U) Ensure implementation of this policy within their Division.
- 11.7.3. (U) Ensure plans for acquisition and use of FOCI software, OSS, and SOUP are coordinated with the AD for Security Division, the FD, the OGC, the contracting officer, and the FBI CIO, as appropriate.
- 11.7.4. (U) Ensure that Systems Administrators within their division do not install or use unauthorized software on FBI systems.
- 11.7.5. (U) With the ISSM and System Administrator, ensure that software holdings are reviewed and plans are developed to eliminate unauthorized software from FBI operational IS.
- 11.7.6. (U) Ensure software acquisitions that are to be used on FBI operational IS is compliant with criteria provided by the AD for Security Division and the FD.
- 11.8. (U) Program/Project Managers for Development and Evaluation Environments must:
- 11.8.1. (U) Ensure that development environments and evaluation environments are isolated from FBI operational systems and FBI sensitive information.
- 11.8.2. (U) Approve the use of OSS and SOUP in the development or evaluation environment that they manage.
- 11.8.3. (U) Ensure compliance with the change control processes for operational FBI IS before moving software from development or evaluation environments to operational FBI IS.
- 11.9. (U) System Administrators must:
- 11.9.1. (U) Ensure that all software installed on FBI IS is authorized software.
- 11.9.2. (U) With the ISSM and Information System Owner, review software holdings and develop plans for elimination of unauthorized software.
- 11.9.3. (U) With the ISSM and the Information System Owner, ensure that new software to be added to an FBI IS is evaluated for compatibility with existing software.
- 11.10. (U) Users must:
- 11.10.1. (U) Use FBI software only for the purposes for which it is authorized.
- 11.10.2. (U) Comply with the FBI Information System Use Policy Directive (0581D).

11.10.3. (U) Report violations of this policy according to SIRS.

## 12. Exemptions:

(U//~~FOUO~~) Software Used for FBI Business performed as under cover operations (UCO) or under cover activities (UCA). Software acquired for use in business that is not be identifiable with the FBI, and covert networks, systems, or operations that are not operating over or through other FBI networks, and cover activities that are not to be identifiable with the FBI are exempt from this policy directive but must be approved through operations plans for those operations or activities.

## 13. Supersession:

(U) None

## 14. References, Key Words, and Links:

### 14.1. (U) References:

(U) Executive Order (EO) 13231, Critical Infrastructure Protection in the Information Age, dated October 16, 2001.

(U) Federal Information Security Modernization Act (FISMA) of 2014.

(U) Standards of Ethical Conduct Regulation, 5 CFR Parts 2635 and 3801.

(U) Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7), Issued December 17, 2003.

(U) NSPD-54/HSPD-23, Cybersecurity Policy, 8 January 2008, and Comprehensive National Cybersecurity Initiative (CNCI) number 11, Develop Multi-pronged Approach for Global Supply Chain Risk Management.

(U) NIPP (Draft v2.0) National Infrastructure Protection Plan, Updated draft released for comment January 20, 2006.

(U) Director of Central Intelligence Directive (DCID) 7/6, Community Acquisition Risk Center, dated March 2, 2005.

(U) Intelligence Community Directive (ICD) Number 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation, dated September 15, 2008.

(U) Committee on National Security Systems Instruction No. 4009 National Information Assurance Glossary €" Revised April 2010

(U) Committee on National Security Systems Report [CNSS-075-03] Foreign Influence on United States Information Technology, dated September 2003.

(U) Committee on National Security Systems Report, CNSS-145-06 Framework for Lifecycle Risk Mitigation for National Security Systems in the Era of Globalization, dated November 2006.

(U) NSTISSP No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, revised June 2003.

(U) National Communications System, Foreign Ownership of U.S. Domestic Telecommunications Infrastructure, dated 03/2001.

(U) DOJ Order 2640.2F, Information Technology Security, 11/26/2008.

(U) FBI Certification and Accreditation Handbook

(U) The FBI Ethics and Integrity Policy Manual of December 6, 2007.

(U) FBI Information Technology (IT) Life Cycle Management (LCM), Version 4.0.1 dated 02/28/2008.

(U) FBI Electronic Record Keeping Certification Manual, April 20, 2004.

(U) FBI IT Life Cycle Management Handbook, September 30, 2008.

(U) Security Assessment and Authorization for FBI Information Systems Policy Directive (0655D)

(U) ASAPU Electronic Communication, 319B-HQ-1487495-FD-Serial 3, Procurement Matters; Finance Division (FD), Advance Procurement Planning, 02/27/2007.

(U) State-of-the-Art Report (SOAR), Information Assurance Technology Analysis Center (IATAC) Data and Analysis Center for Software (DACS), Software Security Assurance, dated 07/31/2007.

(U) Federal Acquisition Regulation, Volume II, Part 52-227.

(U) Federal Acquisition Regulation, Part 27.

### 14.2. (U) Key Words:

FBI Life Cycle Management Directive (LCMD)

FBI IT Life Cycle Management (LCM) Handbook

Foreign Ownership, Control or Influence (FOCI)

Commercial Off the Shelf Software (COTS)

Government Off the Shelf Software (GOTS)

Open Source Software (OSS)

Software of Unknown Pedigree (SOUP)

Software Assurance

Software Acquisition

Software Control

Software Life Cycle

Software Maintenance

Software Management

Software Protection

Software Provenance

### 14.3. (U) Links:

(U) Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Executive Office of the President of the United States, June 2009. (www.whitehouse.gov Internet site).

(U//~~FOUO~~) FBI Cyber National Threat Assessment, June 22, 2009. (~~SECRET//ORCON/NOFORN~~)

(U//~~FOUO~~) CNSS Report on Foreign Influence on U.S. Information Technology, September 2003

(U//~~FOUO~~) The Foreign Intelligence Threat in the United States, December 29, 2006.

(~~SECRET//ORCON/NOFORN~~)

b3

b7E

(U) FBI Community Acquisition Risk Program

a. (U) Supply Chain Risk Management Program

b. (U) Supply Chain Risk Management Process Information Overview

(U) FBI IT Life Cycle Management Handbook

(U) Security Assessment and Authorization Policy Guide, 0655PG

(U) FBI Electronic Record Keeping Certification Manual

(U) FBI Information Systems Use Policy Directive (0581D)

(U) FD Acquisition

(U) SECD Acquisition Security

(U) SIRS

(U) IT licenses

(U) Contracting

(U) IT Acquisition

## 15. Definitions:

15.1. (U) Assurance (Software) - Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime in its supply chain, and confidence that the software performs its functions in the intended manner.

15.2. (U) Acquisition - Acquiring by contract with appropriated funds of supplies or services (including construction) by or and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

15.3. (U) Acquisition Planning - The process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency need in a timely manner and at a reasonable cost. It includes developing the overall strategy for managing the acquisition.

15.4. (U) Certification and Accreditation Process - The process by which an FBI IS is assessed and authorized for operation according to the Security Assessment and Authorization for FBI Information Systems Policy Directive (0655D), including:

a. Certification. Comprehensive evaluation of the technical and nontechnical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. To be renamed the "risk assessment process."

b. Accreditation. - Formal declaration by a Designated Accrediting Authority (DAA) that an IS is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. To be renamed the "authorization process."

15.5. (U) Change Control Process - A process by which a change is proposed, evaluated, approved (or disapproved), scheduled, and tracked. Change control is a method of configuration management, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to work products. Change control includes a systematic proposal, justification, evaluation, coordination, approval or disapproval of proposed changes. The change control process identifies, documents, approve or rejects, and controls changes to project baselines.

15.6. (U) Commercial Software - Copyrighted software sold for profit by businesses. Commercial Software includes Commercial Off-the-shelf software, and special purpose software developed for a particular consumer base.

15.7. (U) Commercial Off the Shelf Software (COTS) - Copyrighted software sold for profit by businesses as a commodity offering.

15.8. (U) Community Acquisition Risk Directorate of the National Counterintelligence Executive (NCIX) for the Director of National Intelligence - The Director of National Intelligence directorate responsible for analyzing the counterintelligence and security threats inherent in proposed Intelligence Community (IC) acquisitions and ensuring that all IC elements conduct a thorough risk assessment of all proposed contracts. Risk assessments will specify threats of contracting with vendors as low, medium, high or critical risk. Effective March 2010, the NCIX/ community acquisition risk section (CARS) became the Acquisition Risk Directorate (ARD) of the NCIX.

15.9. (U) Compatibility - A device or software that can be used with an IS without causing a negative impact on the reliability, integrity, confidentiality, or availability of that IS, its application, or its information.

15.10. (U) Critical Asset - Those assets that process, store, or transmit data that is considered essential to the nation's infrastructure in support of law enforcement, national security, or intelligence activities. Failure or loss of function of a critical asset could cause adverse national impact.

15.11. (U) FBI Sensitive Information - Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Systems that are not national security systems, but contain FBI sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235).

a. FBI sensitive information includes, but is not limited to, information that is exempt from disclosure under the Freedom of Information Act. This includes: proprietary data, ~~For Official Use Only (FOUO)~~ information, treaties and international agreements, technical military data, export control data,

b7E

competition sensitive data, privacy act information, investigative and inquiry data, law enforcement, ~~formerly restricted data (FRD)~~, and naval nuclear propulsion information.

b. FBI sensitive information may also include, but is not limited to, privacy information, Need-to-know (NTK) information, Law Enforcement Sensitive (LES) information, legal compliance information, Personally Identifying Information (PII), Intellectual Property (IP) information, financial information, operating information, contract information, and other information as directed by the FBI.

15.12. (U) FBI Software - Software that is properly acquired by the FBI for purposes related to execution of the FBI mission.

15.13. (U) Foreign Intelligence Entity (FIE) - Foreign Intelligence Services (FIS) and Intelligence Collecting Organizations that are not under control of a Foreign Government.

15.14. (U) Foreign Ownership, Control, or Influence (FOCI) - U.S. company is considered to be under FOCI whenever a foreign interest has the power to direct or decide matters affecting the management or operations of the company in a manner which may result in unauthorized access to National Security Information (NSI), or may adversely affect the performance of a classified contract. Such power may be direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of securities, by contractual arrangements or other means.

15.15. (U) FOCI Software - Software that is developed, distributed, or maintained under Foreign Ownership, Control, or Influence and that will be used to process National Security Information. FOCI software does not necessarily refer to software that was developed by non-US persons or that was developed outside of the United States borders. Much software is developed outside of US borders by non-US persons, but is controlled by a company that is not under FOCI.

15.16. (U) Foreign Influence - Any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States.

15.17. (U) Government Off-the-Shelf (GOTS) - GOTS is a term for software and hardware products that are typically developed by the technical staff of the government agency for which it is created, and includes all in-house developed software. Government Off-the-shelf software is sometimes developed by an external entity, but with funding and specification from the agency. GOTS software solutions can normally be shared among Federal agencies without additional cost.

15.18. (U) Information System Owner - The government officer who serves as the focal point for the information system. In that capacity, the information system owner serves both as an owner and as the central point of contact between the authorization process and the owners of components of the system including, for example:

- a. applications, networking, servers, or workstations;
- b. owners/stewards of information processed, stored, or transmitted by the system; and
- c. owners of the missions and business functions supported by the system. Some organizations may refer to information system owners as program or project managers or business/asset owners.

15.19. (U) Licensing Criteria for Software - The terms of use, distribution, control, and maintenance for software devised by the owner of the software products and agreed to by the users of software products. See [REDACTED]

b7E

15.20. (U) Life Cycle Management (LCM) - A comprehensive framework that describes the management of various processes such as acquisition, development, operations and maintenance, and retirement of FBI IT systems and software products. The entire life cycle process is addressed from the initial recognition of need through the retirement and disposal. LCM uses a series of instruments such as boards, teams, standards, and documents for life cycle governance of FBI IT systems.

15.21. (U) Malicious Code - Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an Information System.

15.22. (U) National Information Assurance Partnership (NIAP) - Joint initiative between the National Security Agency (NSA) and the National Institutes of Standards and Technology (NIST) responsible for security testing needs of both IT consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.

15.23. (U) Open Source License - Open source licenses impose certain obligations on users who exercise these copyright and licensing rights. By definition, Open Source Licenses should contain all clauses listed under Licensing Criteria for Software (see definition 19). While the specific requirements differ among the many different open source licenses, common obligations include making the source code available, publishing a copyright notice, placing a disclaimer of warranty on distributed copies, and giving any recipient of the program a copy of the license.

15.24. (U) Open Source Software - Software that is copyrighted and distributed under a license that provides everyone the right to use, modify and redistribute the source code of the software. The source code and certain other rights normally reserved for copyright holders are provided under a software license that meets the Open Source Software Definition or that is in the public domain. In some cases copyright may be renounced by the copyright holder.

15.25. (U) Operational Information System (IS) - An information system that has been given an Approval to Operate (ATO), or Interim Approval to Operate (IATO), by its authorizing authority through the FBI Information Assurance Certification and Accreditation program.

15.26. (U) Provenance - The history of ownership of a valued object. For software, provenance includes identification of the origin and of all points within the software supply chain at which the software could have been subverted.

15.27. (U) Software of Unknown Pedigree (SOUP) - Software that is developed by unknown people or processes. Software that has no identifiable provenance.

15.28. (U) Software Supply Chain - The sequence of designers, producers, manufacturers, shippers, resellers, and maintainers that create a software product and deliver it to its point of sale, or to a customer.

15.29. (U) System Administrator (SA and SysAdmin) - Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

15.30. (U) Technical Systems - Systems that are under the purview of the EAD-STB including, but not limited to systems that are used for:

- a. interception, collection or electronic surveillance of real-time or near real-time wire or electronic communications evidence or intelligence; or

b7E



b. forensic processing, examination, review, tracking or reporting on tangible or intangible evidence (including stored digital evidence).

15.31. (U) Unauthorized Software - Software that has not been properly acquired or approved for use on FBI operational systems.

15.32. (U) US Government Protected Information (USGPI) Information that either 1) meets the standards for National Security Classification or 2) is unclassified information that does not meet the standards for National Security Classification but is (a.) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (b.) under law or policy requires protection from unauthorized disclosure.

15.33. (U) Version Control - The establishment and maintenance of baselines and the identification of changes to baselines that make it possible to return to the previous baseline.

**16. Appendices, Attachments, and Forms:**

(U) None

**Sponsoring Executive Approval**

**Name:**Michael J. Folmar

**Title:**Assistant Director, Security Division

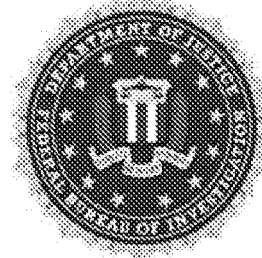
**Final Approval**

**Name:**T.J. Harrington

**Title:**Associate Deputy Director

**UNCLASSIFIED//~~FOUO~~**



UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION  
**POLICY DIRECTIVE**  
**0922D**

<b>1. Policy Directive Title.</b>	(U) Information Systems Use
<b>2. Publication Date.</b>	2016-09-12
<b>3. Effective Date.</b>	2016-09-12
<b>4. Review Date.</b>	2019-09-12

**5. Date of Last Renewal.**

N/A

**6. Authorities:**

- 6.1. (U) National Security Act of 1947, as amended
- 6.2. (U) Intelligence Reform and Terrorism Prevention Act of 2004
- 6.3. (U) Federal Information Security Modernization Act (FISMA) of 2014
- 6.4. (U) The Privacy Act of 1974, as amended, Title 5 United States Code (U.S.C.) Section (§) 552a
- 6.5. (U) Clinger-Cohen Act, repealed and reenacted as 40 U.S.C. § 11101 et seq.
- 6.6. (U) Standards of Ethical Conduct, Title 5 Code of Federal Regulations (CFR) Parts 2635 and 3801
- 6.7. (U) Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*
- 6.8. (U) Department of Justice (DOJ) Order 2640.2F, *Information Technology Security*

**7. Purpose:**

(U) This policy establishes acceptable use requirements for Federal Bureau of Investigation (FBI) information systems. It mandates acknowledgement of the rules of behavior for general and privileged users and the completion of the information security (INFOSEC) awareness and privileged-user security trainings.

**8. Policy Statement:**

- 8.1. (U) FBI personnel must use FBI information systems in strict accordance with the level of access granted by the FBI for authorized purposes and in compliance with all applicable laws, regulations, and policies.
- 8.2. (U) All training required by this policy must be executed annually in accordance with the Training Division (TD) *Mandatory Training and Tracking Policy Directive and Policy Guide*, 0724DPG.
- 8.3. (U) Warning Messages and Banners for FBI Information Systems
  - 8.3.1. (U) FBI information systems, except as noted below in subsection 12.3., must display an approved warning message (also known as a "banner") to users upon login that notifies them of conditions on system use and requires their explicit consent to the monitoring of their communications and online activity for all purposes while using that system. The warning message or banner must remain displayed on the screen, and the user must not be able to access the information system until the user affirmatively acknowledges (or "clicks through") his or her consent to monitoring and acceptance of the conditions. The warning message or banner must:
    - 8.3.1.1. (U) Provide privacy and security notices consistent with applicable federal laws, EOs, directives, policies, regulations, standards, and guidance.
    - 8.3.1.2. (U) Include statements advising personnel that:
      - 8.3.1.2.1. (U) They are accessing a United States government (USG) information system.
      - 8.3.1.2.2. (U) Information system usage may be monitored, recorded, and subject to audit.
      - 8.3.1.2.3. (U) Use of the information system indicates consent to monitoring and recording.
      - 8.3.1.2.4. (U) Unauthorized use of the information system is prohibited. Users who engage in prohibited activity on an FBI information system may be subject to administrative, disciplinary, or security action and criminal and civil penalties.
  - 8.4. (U) Consent to Monitoring and Activity Review
    - 8.4.1. (U) FBI information systems are monitored and accessed for law enforcement, security, counterintelligence, and other compliance purposes. FBI personnel using FBI information systems have no reasonable expectation of privacy for communications transmitted through or data stored on these systems.
    - 8.4.2. (U) By signing the FD-889, "FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form," and/or the FD-889a, "FBI Information Technology and Information Systems Rules of Behavior for Privileged Users Agreement Form," FBI personnel consent to being monitored while using FBI information systems and permitting an aggregated review of their activities on these systems.
- 8.5. (U) Compliance
  - 8.5.1. (U) FBI personnel who do not comply with the requirements set forth in this policy may be subject to adverse administrative, disciplinary, or security action; criminal prosecution; and civil penalties.
  - 8.5.2. (U) Noncompliance with this policy must be reported in accordance with the *Integrity and Compliance Program Policy Guide*, 0814PG. FBI personnel are prohibited from retaliating against any individual who reports a compliance risk in accordance with Policy Directive (PD) 0727D, *Non-Retaliation for Reporting Compliance Risks*. Any misconduct must be reported in accordance with PD 0796D, *Reporting FBI Employee Misconduct*.
- 8.6. (U) FBI personnel must report all known or suspected information system security incidents (ISSIs) in accordance with *Security Compliance Program Policy Guide (0934PG)*.



**9. Scope:**

(U) This policy applies to all FBI information systems and to all general and privileged users of FBI information systems.

**10. Proponent:**

(U) Security Division (SecD)

**11. Roles and Responsibilities:**

11.1 (U) General users must:

11.1.1. (U) Acknowledge reading, understanding, and complying with this policy by signing the FD-889, "FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form," prior to accessing FBI information systems and at least annually thereafter, as well as when required by system changes.

11.1.2. (U) Complete mandatory INFOSEC awareness training in Virtual Academy (VA) within 30 calendar days of being granted initial access to FBI information systems, and at least annually thereafter by the deadline established by the Career Services Management Unit (CSMU), Mission Support Section (MSS), SecD.

11.2. (U) Privileged users must:

11.2.1. (U) Comply with all general-user requirements stated in subsection 11.1.

11.2.2. (U) Acknowledge reading, understanding, and complying with this PD by signing the FD-889a, "FBI Information Technology and Information Systems Rules of Behavior for Privileged Users Agreement Form," prior to being granted privileged access to FBI information systems and at least annually thereafter, as well as when required by system changes.

11.2.3. (U) Complete the privileged-user security training in VA prior to being granted initial privileged access to any FBI information system, and at least annually thereafter by the deadline established by CSMU.

11.3. (U) The assistant director (AD) of SecD, or designee, must:

11.3.1. (U) Make approval decisions for exemptions to this policy.

11.3.2. (U) Ensure that violations of this policy are investigated.

11.3.3. (U) Ensure that INFOSEC awareness training in VA is provided to all general users of FBI information systems, at least annually.

11.3.4. (U) Ensure that privileged-user security training in VA is provided to all privileged users of FBI information systems, at least annually.

11.4. (U) Division/field office (FO) heads must:

11.4.1. (U) Ensure that general users complete INFOSEC awareness training in VA within 30 calendar days of being granted initial access to FBI information systems, and annually thereafter.

11.4.2. (U) Ensure that general users complete INFOSEC awareness training in VA and acknowledge reading, understanding, and complying with the FD-889, "FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form," by the deadline established by CSMU.

11.4.3. (U) Make approval decisions for the reactivation of suspended general-user access to FBI information systems, in coordination with the division's/FO's chief security officer (CSO).

11.5. (U) System owners must:

11.5.1. (U) Ensure that a process exists to deactivate (and reactivate, as necessary) general-user access to FBI information systems for users who fail to complete the INFOSEC awareness training in VA.

11.5.2. (U) Ensure that a process exists to deactivate (and reactivate, as necessary) privileged-user access to FBI information systems for users who fail to complete the privileged-user security training in VA.

11.5.3. (U) Ensure that privileged users complete privileged-user security training in VA and acknowledge reading, understanding, and complying with the FD-889a, "FBI Information Technology and Information Systems Rules of Behavior for Privileged Users Agreement Form," by the deadline established by CSMU.

11.5.4. (U) Initiate, upon notification from the Assurance Management Unit (AMU), IAS, SecD, the deactivation of privileged access to FBI information systems for privileged users who fail to complete the privileged-user security training in VA.

11.5.5. (U) Ensure, in coordination with AMU, that privileged users complete privileged-user security training in VA prior to the reactivation of privileged access to FBI information systems.

11.5.6. (U) Initiate, upon notification from AMU, the reactivation of privileged access to FBI information systems for privileged users who complete the privileged-user security training in VA after privileged access suspension.

11.5.7. (U) Ensure that users of nonenterprise FBI information systems are monitored for compliance with the FD-889, "FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form," and/or the FD-889a, "FBI Information Technology and Information Systems Rules of Behavior for Privileged Users Agreement Form," in coordination with the Enterprise Security Operations Center (ESOC), IAS, SecD.

11.5.8. (U) Ensure that the warning message or banner is displayed to users who attempt to access FBI information systems.

11.6. (U) The Privacy and Civil Liberties Unit (PCLU) of the Office of the General Counsel (OGC) must coordinate with TD and CSMU to ensure that the INFOSEC awareness training in VA includes a privacy component.

11.7. (U) TD must coordinate with PCLU, OGC and CSMU, SecD to ensure that the INFOSEC awareness training in VA includes a privacy component.

11.8. (U) AMU must:

11.8.1. (U) Ensure that privileged users are notified to complete the privileged-user security training in VA by the deadline established by CSMU.

11.8.2. (U) Track completion statistics to provide the following notifications to system owners:

11.8.2.1. (U) Privileged access to FBI information systems that must be deactivated for privileged users who fail to complete the privileged-user security training in VA



11.8.2.2. (U) Privileged access to FBI information systems that must be reactivated for privileged users who complete the privileged-user security training in VA after privileged access suspension

11.9. (U) ESOC must ensure that users of nonenterprise FBI information systems are monitored for compliance with the FD-889, "FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form," and/or the FD-889a, "FBI Information Technology and Information Systems Rules of Behavior for Privileged Users Agreement Form," in coordination with system owners.

11.10. (U) Information system security managers (ISSMs) must:

11.10.1. (U) Make approval decisions for exemption requests from privileged users who are unable to complete the privileged-user security training in VA by the required deadline and ensure that applicable exemption codes are entered in VA for approved exemptions.

11.10.2. (U) Ensure that all exempted privileged users complete the privileged-user security training in VA within 30 calendar days after the exemption is no longer applicable.

11.10.3. (U) Coordinate Section 508 (accessibility) exemptions with the Section 508 program.

11.11. (U) CSMU must:

11.11.1. (U) Establish deadlines for completing INFOSEC awareness and privileged-user security trainings in VA at least annually.

11.11.2. (U) As designated by the AD of SecD, ensure that INFOSEC awareness training in VA is prepared and made available to all general users of FBI information systems at least annually. Notify general users to complete the INFOSEC awareness training in VA by the established deadline.

11.11.3. (U) Ensure that the INFOSEC awareness training in VA includes a privacy component, in coordination with TD and PCLU.

11.11.4. (U) Ensure that privileged-user security training in VA is prepared and made available to all privileged users of FBI information systems at least annually, as designated by the AD of SecD.

11.11.5. (U) Track completion statistics and notify division/FO training coordinators and division/FO CSOs of general users who fail to complete the INFOSEC awareness training in VA.

11.11.6. (U) Provide completion statistics for INFOSEC awareness training and privileged-user security training to the DOJ as required.

11.12. (U) Division/FO CSOs must:

11.12.1. (U) Initiate the deactivation of FBI information system access, upon notification from CSMU, for general users who fail to complete INFOSEC awareness training in VA. The user's supervisor must be notified of the pending deactivation.

11.12.2. (U) Ensure that general users complete the INFOSEC awareness training in VA prior to the reactivation of access to FBI information systems.

11.12.3. (U) Initiate the reactivation of FBI information system access, upon notification from CSMU, for general users who complete the INFOSEC awareness training in VA after access suspension.

11.13. (U) Division/FO training coordinators must:

11.13.1. (U) Make approval decisions for exemption requests from general users who are unable to complete the INFOSEC awareness training in VA by the required deadline. Ensure that the applicable exemption codes are entered in VA for approved exemptions.

11.13.2. (U) Ensure that all users who were granted exemptions complete the INFOSEC awareness training in VA within 30 calendar days after their exemptions expire.

11.14. (U) The Section 508 program must coordinate Section 508-related exemptions with the ISSM.

## 12. Exemptions:

12.1. (U) A general user who is unable to complete the INFOSEC awareness training in VA by the required deadline must submit an exemption request to the division/FO training coordinator. The division/FO training coordinator makes an approval decision based on the exemption criteria in VA and ensures that the applicable exemption code is entered for an approved exemption.

12.2. (U) A privileged user who is unable to complete the privileged-user security training in VA by the required deadline must submit an exemption request to the ISSM. The ISSM makes an approval decision based on the exemption criteria in VA and ensures that the applicable exemption code is entered for an approved exemption.

12.3. (U) FBI information systems used in an approved undercover operation (UCO) and undercover activity locations that are visible to non-FBI personnel are exempt from the warning message or banner requirement in subsection 8.4. See the *Undercover and Sensitive Operations Policy Guide*, 0432PG, for the UCO and undercover activity approval policy and procedures.

12.4. (U) All other requests for exemptions from this policy must be submitted to the AD of SecD or his or her designee.

## 13. Supersession:

(U) PD 0581D, *FBI Information System Use Policy*

## 14. References, Links, and Forms:

14.1. (U) References

14.1.1. (U) Committee on National Security Systems Instruction (CNSSI) No. 4009, *National Information Assurance Glossary*

14.1.2. (U) PD 0533D, *Security Awareness Training and Education (SATE) Program*

14.1.3. (U) PD 0607D, *Security Clearance Requirements for Access to FBI Information Systems*

14.1.4. (U) *Security Compliance Program Policy Guide* (0934PG)

14.1.5. (U) PD 0693D, *Sensitive Compartmented Information (SCI) Access*

14.1.6. (U) PD 0723D, *Federal Bureau of Investigation (FBI) Unclassified Network (UNet) Enclave Policy*

14.1.7. (U) PD 0875D, *FBI Information Systems Privileged User Security Policy*

14.1.8. (U) *FBI Information Systems Use Policy Quick Reference Guide* (QRG)

14.1.9. (U) *Integrity and Compliance Program Policy Guide*, 0814PG

14.1.10. (U) *Mandatory Training and Tracking Policy Directive and Policy Guide*, 0724DPG

14.1.11. (U) *Personnel Security Clearance and Access Policy Guide*, 0192PG

- 14.1.12. (U) [PD 0919D, Accessible Information and Communication Technology \(ICT\), 11/1/2016](#)
- 14.1.13. (U) [Security Assessment and Authorization Policy Guide, 0655PG](#)
- 14.1.14. (U) [The Rehabilitation Act of 1973, 29 U.S.C. § 794d](#)
- 14.1.15. (U) [Undercover and Sensitive Operations Policy Guide, 0433PG](#)
- 14.2. (U) Links
- 14.2.1. (U) [Virtual Academy on the Secret Enclave](#)
- 14.2.2. (U) [Virtual Academy on the Unclassified Enclave](#) [REDACTED]
- 14.2.3 (U) [FBI Accessibility Program Intranet site](#)
- 14.3. (U) Forms
- 14.3.1. (U) [FD-291, "FBI Employment Agreement"](#)
- 14.3.2. (U) [FD-857, "Sensitive Information Nondisclosure Agreement"](#)
- 14.3.3. (U) [FD-868, "Nondisclosure Agreement for Joint Task Force Members, Contractors, Detailees, Assignees, and Interns"](#)
- 14.3.4. (U) [FD-889, "FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form"](#)
- 14.3.5. (U) [FD-889a, "FBI Information Technology and Information Systems Rules of Behavior for Privileged Users Agreement Form"](#)
- 14.3.6. (U) [FD-1001, "Consent for Warrantless Searches of Department of Justice Workplaces"](#)
- 14.3.7. (U) [Form 4414, "Sensitive Compartmented Information Nondisclosure Agreement"](#)
- 14.3.8. (U) [SF-312, "Classified Information Nondisclosure Agreement"](#)

b7E

## 15. Key Words, Definitions, and Acronyms:

- 15.1. (U) Keywords
- 15.1.1. (U) Computer use
- 15.1.2. (U) General user
- 15.1.3. (U) Information system
- 15.1.4. (U) Information system use
- 15.1.5. (U) Information technology
- 15.1.6. (U) Privileged user
- 15.1.7. (U) Rules of behavior
- 15.1.8. (U) Warning banner
- 15.1.9. (U) Warning message
- 15.2. (U) Definitions
- 15.2.1. (U) Accessibility (or accessible): the design of products, devices, services, or environments for people with disabilities. Accessible design ensures both "direct access" (i.e., unassisted) and "indirect access," meaning compatibility with an individual's assistive technology (e.g., computer screen readers).
- 15.2.2. (U) Division/FO heads: includes ADs and heads of FBI Headquarters (FBIHQ) divisions and FOs at a level of authority equivalent to an AD and special agent in charge (SAC).
- 15.2.3. (U) FBI information system: a set of information resources organized for the acquisition, collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information (source: derived from CNSSI No. 4009).
- 15.2.4. (U) FBI personnel: any individual employed by, detailed to, or assigned to the FBI, including interns; task force officers (TFOs); members of the Armed Forces; expert consultants to the FBI; industrial or commercial contractors, licensees, certificate holders, or grantees of the FBI, including all subcontractors or personal services contractors of the FBI; and any other person who acts for or on behalf of the FBI, as determined by the FBI Director.
- 15.2.5. (U) General user: an individual who is authorized to use an FBI information system. For the purposes of this policy, privileged users abide by the responsibilities and requirements of general users (source: derived from CNSSI No. 4009).
- 15.2.6. (U) Information and communication technology (ICT): formerly known as electronic and information technology, ICT includes any information technology, equipment, or interconnected system or subsystem of equipment for which the principal function is the creation, conversion, duplication, automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, reception, or broadcast of data or information. Examples of ICT include, but are not limited to, electronic content (e.g., Web sites, digital files, and electronic documents), software and applications (e.g., Sentinel, Palantir), information technology (IT) services, communication technology products and services (e.g., telephones, voice over Internet Protocol [VoIP] systems, videophones, and smartphones), computers and ancillary equipment (e.g., desktops, laptops, tablets, and peripherals), information kiosks and transaction machines (e.g., the FBI Wall of Honor kiosk), videos and multimedia content (including Webcasts), office equipment (e.g., printers, copiers, scanners, and fax machines), assistive technology and software, and any operational or scientific equipment, tools, or systems.
- 15.2.7. (U) Information system security incident: an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or an imminent threat of violation of security policies, security procedures, acceptable-use policies or standard computer security practices (source: DOJ Instruction 0900.00.01).
- 15.2.8. (U) Privileged user: an authorized individual with access to system control, monitoring, or administrative functions, such as a system administrator, an information systems security officer (ISSO), or a system programmer. A privileged user is any user who has a role that allows that user to use software that gives that user system control, monitoring, or administrative functions. Users with

b7E

elevated privileges with an application or system do not fall under this definition. Examples of privileged users include, but are not limited to:

15.2.8.1. (U) Data administrators who can analyze, classify, and maintain the FBI's data and data relationships and who can configure and reconfigure data repositories and databases and manage user accounts.

15.2.8.2. (U) Identity and access management administrators who can create and modify user profiles, privileges, and access rights of other users.

15.2.8.3. (U) Server administrators who oversee the physical security, integrity, and safety of FBI servers and server farms, can add and modify server software and access other users' accounts, and may be able to change user accounts and authenticators (e.g., passwords).

15.2.8.4. (U) Storage administrators who manage the FBI storage systems, including tapes, disks, and other media, perform backup and recovery operations, and may be able to allocate storage resources to applications.

15.2.8.5. (U) Security administrators who implement FBI INFOSEC policy, can change configuration information, and may be able to modify accounts and authenticators (e.g., passwords).

15.2.8.6. (U) Help desk employees who may temporarily acquire administrative access to personal computers and other resources and to the information these computer resources contain.

15.2.9. (U) Section 508: the specific section within The Rehabilitation Act of 1973, as amended (29 U.S.C. § 794d), that requires the federal government to ensure that the ICT it develops, procures, maintains, or uses complies with the established standards of accessibility (i.e., Section 508 accessibility standards) for individuals with disabilities, unless an exception applies.

15.2.10. (U//~~FOUO~~) Undercover activity: any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another federal, state, or local law enforcement organization working with the FBI (see the *Undercover and Sensitive Operations Policy Guide*, 0432PG).

15.2.11. (U//~~FOUO~~) Undercover operation: an investigation involving a series of related undercover activities over a period of time by an undercover employee (UCE).

(see the *Undercover and Sensitive Operations Policy Guide*, 0432PG).

15.3. (U) Acronyms

15.3.1. (U) AD: assistant director

15.3.2. (U) AMU: Assurance Management Unit

15.3.3. (U) CFR: Code of Federal Regulations

15.3.4. (U) CNSSI: Committee on National Security Systems Instruction

15.3.5. (U) CSMU: Career Services Management Unit

15.3.6. (U) CSO: chief security officer

15.3.7. (U) DOJ: Department of Justice

15.3.8. (U) EO: executive order

15.3.9. (U) ESOC: Enterprise Security Operations Center

15.3.10. (U) FBI: Federal Bureau of Investigation

15.3.11. (U) FBIHQ: Federal Bureau of Investigation Headquarters

15.3.12. (U) FISMA: Federal Information Security Modernization Act

15.3.13. (U) FO: field office

15.3.14. (U) IAS: Information Assurance Section

15.3.15. (U) ISSI: information system security incident

15.3.16. (U) ICT: information and communications technology

15.3.17. (U) INFOSEC: information security

15.3.18. (U) ISSM: information system security manager

15.3.19. (U) ISSO: information systems security officer

15.3.20. (U) IT: information technology

15.3.21. (U) MSS: Mission Support Section

15.3.22. (U) OGC: Office of the General Counsel

15.3.23. (U) PCLU: Privacy and Civil Liberties Unit

15.3.24. (U) PD: policy directive

15.3.25. (U) PN: policy notice

15.3.26. (U) QRG: quick reference guide

15.3.27. (U) SAC: special agent in charge

15.3.28. (U) SATE: security awareness and training education

15.3.29. (U) SecD: Security Division

15.3.30. (U) TD: Training Division

15.3.31. (U) TFO: task force officer

15.3.32. (U) UCE: undercover employee

15.3.33. (U) UCO: undercover operation

15.3.34. (U) UNet: Unclassified Network

15.3.35. (U) U.S.C.: United States Code

15.3.36. (U) USG: United States government

15.3.37. (U) VA: Virtual Academy



**16. Appendices and Attachments:**

(U) None

<b>Sponsoring Executive Approval</b>	
<b>Name:</b>	Laura A. Bucheit
<b>Title:</b>	Assistant Director, Security Division
<b>Final Approval</b>	
<b>Name:</b>	Valerie Parlave
<b>Title:</b>	Executive Assistant Director, Human Resources Branch

**UNCLASSIFIED//~~FOUO~~**



**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.
  - c. Maintain proper physical separation of information systems, wireless devices, PEDs, and other radio frequency (RF) transmitting components from FBI IS operating at different security domains. RF transmitting components must be kept 3 meters from any FBI IS. Unclassified IT/IS must be kept 1 meter from any classified IS.
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 Memorandum (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).
- Corporate Policy Directive 0061D, Consent to Warrantless Search Filing Requirement.
- Corporate Policy Directive 0071D, FBI Information System Use Policy.
- Corporate Policy Directive 0074D, Security Monitoring of FBI Information Systems.
- Corporate Policy Directive 0146D, Personally Owned Storage Media Policy.
- Corporate Policy Directive 0150D, FBI Security Incident Program (SIP) Policy.
- Corporate Policy Directive 0223D, External Security Marking of Information Technology Hardware and Electronic Data Storage Media
- Corporate Policy Directive 0247D, Removable Electronic Storage (RES) Media Protection Policy.
- Corporate Policy Directive 0255D, Video and/or Audio Teleconferencing Policy.
- Corporate Policy Directive 0256D, Portable Electronic Devices (PED) Policy.
- Corporate Policy Directive 0182D, Cross Domain Data Transfer (CDDT) Policy.
- Corporate Policy Directive 0298D, Keyboard, Video and Mouse (KVM) Switches Policy.
- Corporate Policy Directive 0299D, Privacy Policy Implementation Guide.
- Corporate Policy Directive 0335D, Image Capturing Devices within FBI Controlled Facilities Policy.
- Corporate Policy Directive 0388D, Information Systems Security Framework Policy.
- Corporate Policy Directive 0406D, Telework Policy
- Corporate Policy Directive 0504D, Roles and Responsibilities for Reporting a Data Breach
- 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, 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 Program Policy Guide, 0798PG

**FBI Information Technology and Information Systems  
Rules of Behavior for Privileged Users Agreement Form**

**Purpose:** This agreement outlines the acceptable and unacceptable uses of FBI privileged user access to FBI Information Technology (IT) and Information System (IS) resources. The additional access and behaviors required to perform privileged user activities imply the need for enhanced assurance of your competence to perform those activities and of your integrity in their performance. The role of privileged user constitutes a special category of user who can affect and effect the security of FBI IT and IS resources. For that reason, the privileged user agreement includes additional measures to ensure performance integrity and competence.

**Scope:** This agreement applies to anyone who is granted privileged user IT or IS access for any authorized purpose. Privileged users generally maintain the security attributes of users and of technologies for FBI systems and in that regard, privileged users have greater access to FBI IT and IS than does the normal general user.

**Monitoring:** I understand that as a privileged user, all my user activities are subject to monitoring by the FBI. Monitoring may entail an aggregated review of all of my system/network activities and data base entries and activities.

**Statement of Responsibility:** I understand that I am to use my privileged access to FBI systems for lawful, official use and authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations) and as further outlined in this document and other FBI policy directives. Even where granted access, I must only access the privileged user function 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 Privileged Users.

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.

**Access:** Privileged user access to FBI IT/IS, networks, and other agency systems operating in FBI spaces is granted for official and authorized purposes as set forth in the FBI Privileged User Program Policy and Title 5 CFR parts 2635 and 3801 (Federal Ethics Regulations) and as further outlined in this agreement.

**Revocability:** Privileged user access is a revocable privilege. Privileged user access may be revoked as a result of negative findings in official investigations of privileged user access. Failure to sign this form is grounds for revocation of privileged user access.

**Rules of Behavior:** As a Privileged User of FBI IT/IS, I will:

1. Abide by the provisions of the FBI IT/IS Rules of Behavior for General Users except those variations required to perform authorized privileged user activities.
2. Limit the performance of privileged user activities to my privileged user account(s).
3. Consent to monitoring and search of any IT/IS equipment that I use while in or bring into or remove from FBI owned, controlled, or leased facilities.
4. Complete FBI Privileged User Security Training.
5. Successfully complete any technical or administrative training required by the Head of my Division that is related to competent and secure operation of IT and IS for which I have

- privileged user status.
6. Submit to additional investigation and monitoring of my privileged user activities as required to ensure integrity of my privileged user activities. This includes random monitoring of my activities and random polygraphs related to my privileged user activities.
  7. Immediately report any anomalous incident, including errors and oversights related to my privileged user activities, to my Information System Security Officer (ISSO), Information System Security Manager (ISSM), or Chief Security Officer (CSO) according to the appropriate FBI Incident Response Plan.
  8. Use my privileged user role and access to perform only authorized privileged user activities for the benefit of the FBI.
  9. Protect my "root" or "super user" account including passwords and privileges at the highest level of data that it secures.
  10. Change my privileged user account password every ninety (90) days or as required for security reasons.
  11. Protect all output whether hard-copy, electronic, or optical according to FBI policy.
  12. Perform virus and integrity scanning of any media that is to be used to transfer information into an FBI system.
  13. Notify the ISSO when my privileged user access to the system is no longer needed (e.g. transfer, termination, leave of absence, or for any period of extended non-use). If I am an ISSO, then I will notify my CSO when my privileged user access is no longer needed.

**Expressly Prohibited Behavior:** Unless required as part of my official duties as a Privileged User of FBI IT/IS, I will not:

1. Share my privileged user access or privileges with any unauthorized person.
2. Use my privileged user access or privileges to "hack" any IT/IS (networked or non-networked).
3. Attempt to gain access to data for which I am not specifically authorized, to include e-mail and users files in their home directories.
4. Use my privileged user access for non-Government business.
5. Introduce any software or hardware that has not been approved through the FBI Change Management Process into FBI IT/IS, systems or networks.
6. Use any FBI communications, transmission, processing, or storage components for unauthorized purposes.
7. Disclose, without authorization, any personally identifying information (PII) that I access or learn as a result of my privileged user duties and activities.
8. Disclose, without authorization, any sensitive, classified, or compartmented FBI information that I access or learn as a result of my privileged user duties and activities.

**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 13478, which permits the collection of social security numbers.

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 privileged access to FBI IT/IS that operate in FBI space.

The information on this form may be shared with DOJ components and 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 privileged user rules of behavior for accessing FBI information and IT/IS's that operate in FBI space, you may not be permitted such access 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.



**Acknowledgement**

I acknowledge that I have read and understand the above listed Privileged User Rules of Behavior. I also state that I will adhere to these Privileged User Rules of Behavior and that failure to do so may constitute a security violation resulting in denial of privileged user access to FBI IT/IS networks or facilities. I also understand that violation of these Privileged User Rules of Behavior will be reported to the appropriate authorities for further administrative, civil or criminal disciplinary action deemed appropriate.

Printed Name: \_\_\_\_\_ Date: \_\_\_\_\_

Employee Signature: \_\_\_\_\_ Last Four of SSN: xxx-xx- \_\_\_\_\_

FBI Division: \_\_\_\_\_ System Name: \_\_\_\_\_

FBI Personnel File Number (if known): \_\_\_\_\_

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

**Filing Instructions:** Completion of the FBI's annual Privileged User 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: Information Assurance Section, FBI SecD

## References:

- Standards of Ethical Conduct Regulation (5 CFR Parts 2635 and 3801).
- The Federal Information Security Management Act (FISMA) of 2002.
- US Code, Title 18, Section 798, Disclosure of Classified Information.
- Department of Justice (DOJ) Order 2640.2F, Information Technology Security.
- DOJ IT Security Standards.
- Corporate Policy Directive 71D, FBI Information Systems Use Policy.
- Corporate Policy Directive 74D, Security Monitoring of FBI Information Systems.
- Corporate Policy Directive 213D, FBI Information System Privileged User Program Policy.
- 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.
- FD-889, FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form.
- FD-1001 Consent for Warrantless Searches of Department of Justice Workplaces.
- SF-312, Classified Information Nondisclosure Agreement.
- Form 4414, Sensitive Compartmented Information Nondisclosure Agreement.

## Rules of Behavior Agreement for Unclassified FBI-owned Mobile Devices (FD-889b)

**Purpose:** This agreement outlines the signer's responsibilities regarding acceptable and unacceptable uses of any unclassified FBI-owned mobile device.

**Scope:** This agreement applies to all FBI personnel, including FBI employees, interns, detailees, contractors, and approved foreign nationals who are issued an unclassified FBI-owned mobile device.

**Monitoring and Search Notification/Consent:** I consent to the search of the FBI-owned mobile device provided to me as authorized by law and as described below. I also give consent to any telecommunications provider providing service for the FBI-owned mobile device provided to me to disclose to the FBI the content of all text messages sent or received using that mobile device. I understand that a complete search will include, but not be limited to, a search for electronically stored data (including but not limited to links, photo and image files, data files, text messages, and chats), metadata, deleted data, application data, log files, content of communications, and registry files but will exclude interception of voice communications and the activation of the camera or microphone without proper legal process. I give permission for this search, freely and voluntarily and not as the result of any threat or promise of any kind.

I understand that the searches are for the purpose of ensuring compliance with security standards and to aid investigations into possible violations, to include criminal and national security violations. I understand that the searches may be conducted by FBI or Department of Justice security personnel and/or by law-enforcement agents or their designees, including agents of the FBI, and that information obtained from these searches may be used in administrative, disciplinary or criminal proceedings against me or others. When asked by authorized personnel, I will immediately provide access to all FBI-owned mobile devices issued to me. I also understand that FBI-owned mobile devices may be monitored or otherwise accessed for law enforcement, security, counterintelligence, or other compliance purposes (including location data and text messages), but this monitoring capability excludes the interception of voice communications and the activation of the camera or microphone without proper legal process. My agreement to these FBI Rules of Behavior (ROB) constitutes my consent to be monitored, to allow access to all FBI-owned unclassified mobile devices accessed by me, and to permit an aggregated review of all of my activities.

**Statement of Responsibility:** I understand that I am responsible for all activity on the FBI-owned mobile devices provided to me. I am not responsible for any activity on the FBI-owned mobile devices provided to me that is beyond my control (i.e. after device has been reported stolen or if it has been compromised by an attack outside my control). I further understand that I am to use FBI mobile devices for lawfully authorized purposes only, 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. I understand that it is my responsibility to maintain current knowledge of the FBI mobile devices policies and Rules of Behavior.

**Revocability:** The ability to retain and use an FBI-owned mobile device is a revocable privilege.

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

1. Use FBI-owned mobile devices for official business, authorized purposes, and de minimis personal use only. FBI-owned mobile devices are for use by FBI personnel only (no spouse or relative), and must only connect through an authorized FBI network or through secure methods described below when accessing the Internet.
2. Follow the provisions set forth in the Mobile Devices and Mobile Applications Policy Guide 0879PG, or successor, for entry and use of mobiles device in FBI-controlled facilities.
3. Use FBI-owned mobile devices in accordance with the Telework Policy 0406D and Remote Access for General and Privileged Users Policy Guide 0655PG-4, or their successors, when working and/or accessing FBI information remotely.

**Rules of Behavior Agreement for Unclassified  
FBI-owned Mobile Devices (FD-889b)**

4. Use unclassified FBI-owned mobile devices for unclassified information only. Ensure any information created, received, transmitted, or stored on FBI-owned mobile devices is properly marked, and safeguarded in accordance with its appropriate dissemination caveats.
5. When accessing, storing, processing, or transmitting personally identifiable information (PII) using FBI-owned mobile devices:
  - a. Disclose PII in accordance with appropriate legal authorities and the Privacy Act of 1974; and
  - b. Notify supervisor and chief security officer (CSO) immediately in the event of a breach to PII and comply with reporting requirements in the Security Incident Program Policy Guide 0934PG, or successor.
6. Download and install only FBI authorized applications (apps) and software on FBI-owned mobile devices from only FBI authorized sources using only FBI Information Systems (IS).
7. Limit Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages, i.e., texts, to unclassified information.
8. Use FBI-owned mobile devices in accordance with the voice and data consumption criteria established by systems owners.
9. Install only FBI-provided removable media, to include memory and subscriber identity module (SIM) cards, on FBI-owned mobile devices.
10. Ensure any Wi-Fi connections use a WPA2 password protected secure wireless network, at a minimum.
11. Complete FBI mobile device awareness training annually.
12. Maintain possession of FBI-owned mobile devices and adhere to the requirements set forth in the Mobile Devices and Mobile Applications Policy Guide 0879PG, and in the FBI Ethics and Integrity Program Policy Directive and Policy Guide 0754DPG, or their successors. Do not leave FBI-owned mobile devices unattended. Lock and securely store FBI-owned mobile devices to prevent unauthorized handling or access (e.g., USG-approved container/safe/locker, locked vehicle, or residence). Do not use hotel safes to store FBI-owned mobile devices. Additionally:
  - a. Report all known or suspected security incidents, to include lost or stolen FBI-owned mobile devices, or improper use of FBI-owned mobile devices, according to the Security Incident Program Policy Guide 0934PG, or successor, and submit a Security Incident Reporting System (SIRS) report within EPAS.
  - b. Report lost or stolen FBI mobile devices to the Enterprise Operations Center (EOC (202-324-1500) immediately.
13. Upload all information created, transmitted, and/or stored on FBI-owned mobile devices that meet the definition of a non-transitory federal record into Sentinel.
14. Preserve all relevant emails and text messages in accordance with the Preservation and Disclosure of Electronic Communications in Federal Criminal Cases Policy 0423D, or successor, if a recipient of litigation holds notice and used a FBI-owned mobile device to receive, create, transmit, or store information related subject matter of the litigation hold. For all other types of relevant electronically stored information (i.e., photographs or videos), contact the Office of the General Counsel's (OGC) Discovery Coordination and Policy Unit.
15. Follow the requirements set forth in the Government Vehicle Use Policy Guide 0791PG or successor when operating government vehicles while in possession of FBI-owned mobile devices.

<p align="center"><b>Rules of Behavior Agreement for Unclassified FBI-owned Mobile Devices (FD-889b)</b></p>
------------------------------------------------------------------------------------------------------------------

16. Complete the FD-772 – Report of Foreign Travel, adhere to Mobile Devices and Mobile Applications PG 0879PG, or successor, while traveling in a foreign nation with an FBI-owned mobile device. Additionally, while on foreign travel:

a. Only connect devices to Wi-Fi networks or hotspots controlled and maintained by the USG where the security setting is at a minimum of WPA2.

b. *High- or critical-threat countries*: Disable Bluetooth, NFC, and GPS capabilities.

c. *Low- or moderate-threat countries*: Disable Bluetooth and NFC. Enable GPS and other location-tracking capabilities, unless there is an operational need to disable location services.

**Expressly Prohibited Behavior:** Unless required as part of official duties, the following are prohibited:

1. Use of Internet Cafes or other public / "shared-key" Wi-Fi locations to conduct official business.

2. Use of mobile sharing technologies/Near Field Communication (NFC) technology (which establishes communication between devices when they touch) is prohibited other than when communicating between government furnished devices (FBI and other agencies). Use of mobile sharing technologies is prohibited within FBI controlled facilities.

3. Use of FBI-owned mobile devices with other IT devices, unless authorized by the FBI Authorizing Official (AO). If authorized for use with other IT devices, the FBI-owned mobile device cannot store United States Government Information (USGI) or PII in any capacity.

4. Use of proxies to obscure personal activities or identities, unless there is an authorized operational need.

5. Alter, change, configure, install software or hardware, or connect IT or systems or otherwise tamper with any FBI-owned mobile device. This includes installing prohibited applications or tampering with the mobile device to allow the installation of prohibited applications.

6. Use FBI-owned mobile devices for profit-making, commercial activities, or for purposes that are prohibited or reflect adversely on the FBI (e.g., accessing pornography; promoting supremacist or racist causes, selling products or services online, gambling, or similar activities).

7. Use FBI-owned mobile devices to access social media on an FBI-owned mobile device is expressly prohibited except for operational purposes, according to the Social Media and Other Electronic Information Sharing Technologies Policy Directive and Policy Guide, 0579DPG, or its successor.

8. Port, transfer, or forward mobile telephone numbers (MTNs) or other lines of communication to non-FBI-owned devices or accounts (e.g., call forwarding from an FBI-owned mobile phone to a personally owned mobile phone). Similarly, FBI personnel are prohibited from forwarding non-FBI-owned MTNs to FBI-owned mobile devices.

9. While on foreign travel with an FBI-owned mobile device:

a. Perform over-the-air (OTA) firmware updates to their devices (or operating systems), unless stationed OCONUS or otherwise directed by systems owners.

b. Connect FBI-owned mobile devices to any devices that are not FBI-owned (e.g., public computer, public wall charger, or airport charger) or otherwise approved by systems owners for data transfer or power charging.

c. Download, install, or update mobile apps from public and/or private mobile app stores, unless directed by systems owners.

d. *High- or critical-threat countries*: use of external storage/removable media, and the media must be removed prior to travel.

e. *Low- or moderate-threat countries*: connect devices to public, unsecured, or "shared-key" Wi-Fi networks or hotspots, even if secure protocols like WPA2 are in place.

**Rules of Behavior Agreement for Unclassified  
 FBI-owned Mobile Devices (FD-889b)**

**Acknowledgment:** I acknowledge that I have read and understand the above listed Rules of Behavior. I will adhere to these Rules of Behavior and I acknowledge that failure to do so may constitute a security violation that could result in denial of access to FBI-owned mobile devices, FBI IT and information systems and networks, or FBI controlled 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, as deemed appropriate.

User's Name (*print*): \_\_\_\_\_

Personnel File ID: \_\_\_\_\_

User's Signature/Date: \_\_\_\_\_

**MOBILE DEVICE INFORMATION**

Property # (if applicable): \_\_\_\_\_ Mobile Telephone #: \_\_\_\_\_

Make & Model: \_\_\_\_\_ UNet E-Mail: \_\_\_\_\_@ic.fbi.gov

Serial #: \_\_\_\_\_

**Filing Instructions:** A copy of the Acknowledgement (this page) must be provided to the user's mobile device POC, and uploaded into the user's official personnel file in Sentinel. The annual completion of FBI INFOSEC awareness training satisfies the annual recertification signatory and acknowledgement requirements for the purpose of storage and audit of this form.