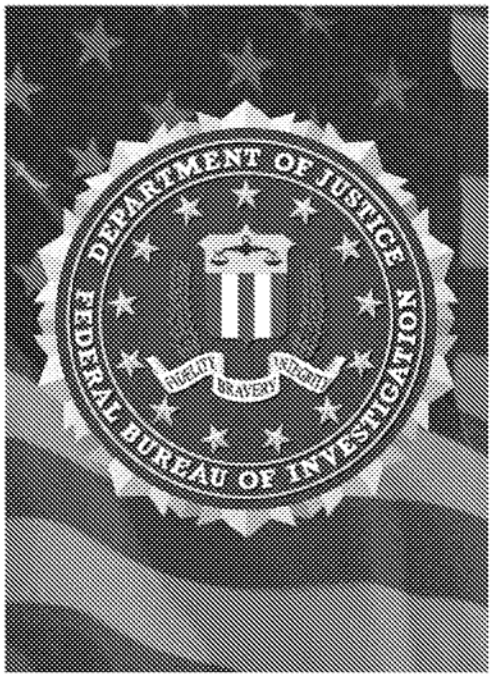
Mobile Devices and Mobile Applications Policy Guide



Federal Bureau of Investigation

Office of the Chief Information Officer

1119PG

November 20, 2020

Approvals

Policy Information	
Last Updated	N/A
Effective Date	2020-11-20
Review Date	2023-11-20
Approval Information	
Sponsoring Executive Approval	**Jonathan C. Moffa** Acting Assistant Director Office of the Chief Information Officer
Final Approval	**Paul M. Abbate** Associate Deputy Director

General Information

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

Federal Bureau of Investigation Headquarters (FBIHQ)

Office of the Chief Information Officer (OCIO)

Policy point of contact: SecD division policy officer (DPO) [redacted] or Mobility Program Office (MPO) unit chief [redacted] b7E

Supersession Information

This document supersedes the *Mobile Devices and Mobile Applications Policy Guide* (1061PG).

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.

Revision Log

The revision log documents substantive changes made to the previous version of this policy, the *Mobile Devices and Mobile Applications Policy Guide* (1061PG), published on July 24, 2019. The numbers and titles in the "Revised" column refer to the subsections as they currently appear in this updated policy. "Deleted" subsection numbers refer to those in the previous published version of the policy.

Revised Section Number and Title	Deleted Section Number and Title
3.3.1. Personally Owned Mobile Devices	
4.3.2.1. *De Minimis* Personal Use	
4.3.2.2. Unauthorized Use	

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 3
1.5. Exemption 3
2. Roles and Responsibilities 5
2.1. Executive Assistant Director (EAD), Information Technology Branch 5
2.2. Authorizing Official (AO) 5
2.3. Assistant Director (AD), Security Division (SecD) 5
2.4. Systems Owners 6
2.5. Mobility Program Office (MPO), Collaboration and Identity Services Section (CISS), Information Technology Infrastructure Division (ITID) 7
2.6. Enterprise Information Security Section (EISS), Office of the Chief Information Officer 7
2.7. Information Security Workforce Services Unit (ISWS), Enterprise Information Security Section, Office of the Chief Information Officer 7
2.8. Enterprise Security Operations Center, ITB 7
2.9. Career Services Management Unit (CSMU), Strategic Resources Section (SRS), Security Division 8
2.10. Section Chief, Security Operations Section (SOS), Security Division 8
2.11. Physical Security Unit, Security Operations Section, Security Division 8
2.12. Accounts Receivable Unit (ARU), Accounting Section (AS), Finance Division 8

2.13. Asset Management Unit, Accounting Section, Finance Division 8
2.14. Procurement Section, Finance Division 8
2.15. Insider Threat Office 9
2.16. Internal Investigations Section, Inspection Division 9
2.17. FBI Accessibility Program, Office of the Chief Information Officer 9
2.18. Digital Forensics and Analysis Section (DFAS), Operational Technology Division (OTD) 9
2.19. Technically Trained Agent Operations and Development Unit (TODU), Field Operations Section (FOS), Operational Technology Division 9
2.20. Training Coordination and Support Unit (TCSU), Training Services Section (TSS), Training Division 9
2.21. Creative Media Development Unit (CMDU), Curriculum Management Section, Training Division 10
2.22. Office of the General Counsel 10
2.23. Office of Integrity and Compliance (OIC) 10
2.24. Program Manager 10
2.25. FBI Headquarters Division or Field Office Heads 10
2.26. Mobility Point of Contact 11
2.27. Enterprise Requirements and Capabilities Working Group (ERCWG) 11
2.28. Property Custodian 11
2.29. Chief Security Officer (CSO) 11
2.30. FBI Personnel 12
3. Policy Statement 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 15
3.4. Installation and Use of Signal Enhancement Devices 15
3.5. Security Incidents 15
3.6. Search and Seizure 16
3.7. Policy Compliance 17
4. Processes and Procedures 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 24
4.3.7. Use with Other Information Technology Devices 24
4.3.8. Use of FBI-Owned Mobile Devices While Operating Government Vehicles 27
4.3.9. Transport and Storage 27
4.3.10. Foreign Travel 28
4.3.11. Software and Hardware Installation or Modification 31
4.3.12. Issuance, Maintenance, and Replacement of FBI-Owned Mobile Devices 31
4.3.13. Device Return 31
4.4. Management and Configuration of FBI-Owned Mobile Devices 32
4.4.1. Acquisition 32
4.4.2. Section 508 32
4.4.3. Asset Management 32
4.4.4. Security Assessment and Authorization 32
4.4.5. Marking 32
4.4.6. Configuration 32
4.4.7. Encryption 33
4.4.8. Malware Protection 33
4.4.9. Service Management 33
4.4.10. Mobile Application Management 33
4.4.11. Mobile Infrastructure 33
4.4.12. Foreign Travel Device Configuration 34

4.4.13. Remote Administration 35
4.4.14. Collection of Data Analytics 35
4.4.15. Sanitization and Destruction 35
4.5. Exemptions and Exceptions 35
5. Authorities 37
5.1. Federal 37
5.2. Intelligence Community Directives (ICD) 37
5.3. Committee on National Security Systems (CNSS) 37
5.4. Department of Justice 37
6. Recordkeeping Requirements 38

List of Appendices

Appendix A: References A-1
Appendix B: Definitions and Acronyms B-1
Appendix C: Security Controls Policy Reference Matrix C-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 26
Table 3: Connection of Unclassified FBI-Owned Mobile Devices to other Unclassified FBI-Owned IT Resources 27

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) 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.
- 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.

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.

1.5. Exemption

Mobile devices containing digital evidence are exempt from this PG. Refer to the *Digital Evidence Policy Guide* (0830PG) for more information.

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.

Mobile devices owned by emergency medical technicians (EMT) are exempt from this PG.

Court-ordered personal monitoring devices are exempt from this PG.

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.

2.2. Authorizing Official (AO)

The FBI Authorizing Official (AO) or designated individual or body 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 with SecD concurrence.
- Ensure that a process is established and published for the acquisition or custom development of mobile apps for FBI-owned 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. If the deviation usage impacts the accreditation of secure space, concurrence must be obtained from the accrediting official (SecD/SOS/Physical Security Unit [PSU] unit chief [UC]).
- 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.
- Maintain internal waiver documentation.

2.3. Assistant Director (AD), Security Division (SecD)

The AD of SecD must:

- Ensure the security requirements of this PG are supported through FBI security programs.

- Ensure the security violations of this PG are investigated and sanctions are enforced, when appropriate.

2.4. Systems Owners

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

- The Enterprise Security Operations Center's (ESOC) security requirements on FBI-mobile devices are reviewed, accepted, and implemented.
- Their mobile devices comply with the *Legal Hold Policy Directive* (0619D), including data preservation and deletion suspension requirements.
- 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.
- The rules of behavior for FBI-owned mobile devices are developed and maintained in coordination with the Enterprise Information Security Section (EISS) of the Office of the Chief Information Officer (OCIO) 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 ESOC 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.
- 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 information and 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.

2.5. Mobility Program Office (MPO), Collaboration and Identity Services Section (CISS), Information Technology Infrastructure Division (ITID)

The MPO must:

- Perform the system-owner responsibilities for enterprise mobile devices, as assigned by the FBI CIO.
- Track and maintain documentation reflecting the status of all enterprise mobile application requests, reviews, and approval decisions.
- Present a "terms of use" (ToU) agreement to users prior to the deployment and installation of any custom mobile apps designed for use on enterprise mobile devices, notifying the user of any restrictions established during the request process and detailing the applicable privacy policy.
- Ensure the SecD accrediting official concurs with restrictions that may impact the technical integrity of secure spaces and Sensitive Compartmented Information Facilities (SCIF).

2.6. Enterprise Information Security Section (EISS), Office of the Chief Information Officer

The SC of the EISS must provide guidance related to the use of mobile devices within FBI-controlled facilities and coordinate with other sections or other divisions, as necessary.

2.7. Information Security Workforce Services Unit (ISWS), Enterprise Information Security Section, Office of the Chief Information Officer

The UC of IT Security Workforce Unit must:

- Provide guidance to systems owners on the system security protocols and use of mobile devices on FBI information.
- Perform a compliance assessment in accordance with the Information Assurance (IA) Policy Compliance Assessment Plan.

2.8. Enterprise Security Operations Center, ITB

The ESOC must ensure that:

- 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 Office (InTO) 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.

2.9. Career Services Management Unit (CSMU), Strategic Resources Section (SRS), Security Division

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

2.10. Section Chief, Security Operations Section (SOS), Security Division

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

2.11. Physical Security Unit, Security Operations Section, Security Division

The PSU UC (also known as the accrediting official) of SecD must:

- Approve or deny exemption requests related to the entry and use of mobile devices into FBI-controlled facilities and coordinate with other sections within SecD, as necessary.
- Identify, publish, and maintain restrictions regarding the entry and use of mobile devices in FBI-controlled facilities.
- Provide guidance to operators on the proper rules of behavior for FBI-owned mobile devices.

2.12. 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.

2.13. 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.
- Make approval decisions for exemption requests regarding the asset management of FBI-owned mobile devices.

2.14. 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.

2.15. Insider Threat Office

The InTO 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.

2.16. Internal Investigations Section, Inspection Division

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

2.17. FBI Accessibility Program, Office of the Chief Information Officer

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.

2.18. 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* (0830PG).
- Perform all forensic examinations of FBI mobile technologies, mobile apps, and infrastructure, as described by the *Digital Evidence Policy Directive and Policy Guide* (0830PG).

2.19. Technically Trained Agent Operations and Development Unit (TODU), Field Operations Section (FOS), 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.

2.20. Training Coordination and Support Unit (TCSU), Training Services Section (TSS), Training Division

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

2.21. 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.

2.22. Office of the General Counsel

The OGC must:

- Provide legal input and requirements to systems owners, the MPO, and the ESOC concerning FBI-owned mobile devices, including, but not limited to, the rules of behavior.
- Provide legal reviews, including privacy and discovery assessments, of mobile apps used with FBI-owned mobile devices.

2.23. Office of Integrity and Compliance (OIC)

The OIC must:

- Provide ethics and standards of conduct advice to systems owners and users regarding the rules of behavior for FBI-owned mobile devices.
- Provide ethics and standards of conduct training while using FBI-owned mobile devices in accordance with the *FBI Ethics and Integrity Program Policy Guide* (1120PG).

2.24. Program Manager

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

2.25. FBI Headquarters Division or Field Office Heads

FBIHQ 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.
- 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 in coordination with MPO.
- Initiate payment requests, upon receiving notification of instances of excessive usage from the MPO, to FBI personnel responsible for incurring unauthorized charges. FBIHQ 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.
- Refer instances of inappropriate or unauthorized use of FBI-owned mobile devices to INSD and/or SecD, Analysis and Investigations Unit (AIU), as deemed appropriate.
- Suspend, remove, revoke, and/or reallocate enterprise mobile devices, as deemed appropriate, and in accordance with this PG (e.g., if there is a significant instance of inappropriate or unauthorized use).

2.26. 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.

2.27. Enterprise Requirements and Capabilities Working Group (ERCWG)

The ERCWG must review enterprise custom and commercial mobile application requests submitted directly to them or advanced to them by the Mobile Applications Review Committee (MARC). When designated authority by the AO, the ERCWG will make mobile application approval or denial decisions based upon its review. The process for this review is contained in the Mobile Applications Review Process and ERCWG Charters.

2.28. Property Custodian

The property custodian of a division or an FO must:

- Meet acquisition and asset management requirements for FBI-owned mobile devices.
- Maintain the receipt of government property forms for users of FBI-owned mobile devices.

2.29. 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 SCIFs.
- 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. The mitigations and device information must be fully documented. Waivers of a temporary duration may be approved by the CSO. Anything longer must be approved by SecD, PSU.
- Execute enterprisewide actions on enterprise mobile devices and applications, as directed by, and in coordination with, the MPO and/or the ESOC (e.g., performing OS updates, uninstalling mobile applications which are not approved for use, etc.)

2.30. 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.
- 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 *Self-Reporting Requirements Policy Guide* (1037PG), 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 the *Encryption of Electronic FBI Information Policy Directive* (0592D).

3. Policy Statement

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 should 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 to overt sites.
    - 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) via the Office 365 (O365) application (via www.324anywhere.com) when teleworking, as long as FBI information is not downloaded to the personal device. 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. Employees must exercise caution when accessing official information pursuant to these exceptions. Among other things, improper transfer of official information to personal devices (even if inadvertent) can result in personal devices becoming discoverable and subject to production in civil and criminal cases. Furthermore, FBI personnel may not use personal accounts (such as Gmail) for official business, except as described in DOJ Policy Statement 801.04, *Electronic Mail and Electronic Messaging Records Retention* (approved on December 11, 2019).

Any violation of these guidelines must be reported under subsection 4.1. of the *Self-Reporting Requirement Policy Guide* (1037PG).

Rules governing the *de minimis* use of FBI mobile devices are described in subsection 4.3.2.1.

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:

- 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 *Memorandums of Understanding and Noncontractual Agreements Policy Guide* (1031PG). 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 Policy Guide* (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).

3.6. 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.

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 Guide* (0830PG).

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 Policy Guide* (0934PG). Based upon the classification or sensitivity level of the information, the device may also be sanitized in accordance with the *Destruction of Classified and Sensitive Material Policy Directive* (0506D).

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.

3.7. 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 the *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 EISS at least every two years.

4. Processes and Procedures

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[1,2,3,4,5]	No[3,4,5,6,7,8]
Mobile devices without wireless, speakerphone, photographic, audio/video recording, or video call/chat capabilities	Yes	Yes[8]

Notes

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.

2: Use of speakerphone, photographic, audio/video recording, or video call/chat capabilities on non-FBI-owned mobile devices is prohibited.

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, *Video and Audio Teleconferencing (VTC)*.

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.

5: Visitors must be notified of mobile device provisions prior to their arrival.

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.

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.

8: OGA-owned laptops must be approved by the appropriate CSO prior to entry and use. See subsection 4.1.2. regarding approvals.

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 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 [redacted] 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

Any mobile device, including a personally owned device not intended for covert operations, must be powered off within three miles of travelling to or from known undercover locations.

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 any required training, at least annually, that includes the following:

- Mobile device and mobile app security awareness
- 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

In accordance with the Standards of Ethical Conduct for Employees of the Executive Branch, "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, employees may use government property only for official business or as authorized by the government, which includes *de minimis* personal use of FBI-owned mobile devices. *De minimis* in this context means that the use must:

1. Involve a negligible expense to the FBI.
2. Not adversely affect the performance of official duties.
3. Be of minimal duration and frequency.

Even if the use is *de minimis* in nature, FBI property and/or time may not be used for profit-making or commercial activities or for purposes that are prohibited or reflect adversely on the FBI, such as:

1. Accessing pornography.
2. Promoting supremacist or racist causes.
3. Selling products, including personal items, or services (except on authorized bulletin boards).
4. Gambling.
5. Sending or forwarding chain e-mails.
6. Engaging in partisan political activities.
7. Engaging in activity (e.g., sending personal messages) involving unprofessional conduct. Unprofessional conduct is defined as conduct—on or off duty—that dishonors, disgraces, or discredits the FBI; seriously calls into question the judgment or character of the employee; or compromises the employee's standing among his or her peers or community. See the FBI's Offense Codes and Penalty Guidelines.

Use of personally owned mobile devices is addressed in subection 3.3.1.

4.3.2.2. Unauthorized Use

As outlined in subsection 4.3.2.1., FBI-owned mobile devices must not be used for personal reasons, even if *de minimis*, if they fall under categories 1–7 or similar activities. Accessing 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).

FBI personnel are expected to adhere to the requirements in this PG and those in the *FBI Ethics and Integrity Program Policy Guide (1120PG)* and the *Public Affairs Policy Guide: Media Relations, External Communications, and Personal Use of Social Media* (1002PG) 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 Guide (1120PG)*, regardless of whether or not the use occurs during their scheduled working hours. 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

FBI personnel, per assigned line, per month, are allocated a specific amount of data consumption and/or peak-usage minutes. These allotments vary pursuant to the most current carrier contract(s) and may be found on MPO's BuNet page, which is updated regularly.

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 mobile POC 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 if such a charge is determined to be appropriate by division supervisory personnel in the offender's chain of command. FBI personnel must provide payments to the ARU of FD with any supporting documentation.

FBI personnel expecting to exceed the current allotment of data consumption or peak-usage minutes as identified in MPO's BuNet page 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. b7E

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 may 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 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 applicable terms of use and the rules of behavior for the device, as outlined in the FD-889b "Rules of Behavior Agreement for Unclassified FBI-owned Mobile Devices" form.

4.3.5.1. Requesting Mobile Applications for Enterprise Mobile Devices

Requests for mobile apps to be used on enterprise devices must be submitted through the approved Mobile Application Review Process (detailed in the Mobile Application Review Process Charter). The Mobile Application Review Process entails a formal review of privacy, discovery, security, and ethics considerations by cross-divisional teams of interested stakeholders. The Mobile Applications Review Process must be instituted, documented, maintained, and regularly reviewed by the MPO, in conjunction with SecD and OGC.

Mobile apps will require security screenings prior to approval. Even if approved, mobile applications may be removed from the approved list if security, operational, legal, or ethical concerns about the mobile applications arise.

Requestors may appeal a rejection following the initial screening of a mobile application request or a rejection by MARC, so long as the mobile application serves a business purpose, and the requestor obtained written approval to appeal from the requestor's SC or ASAC. (See the Mobile Application Review Process Charter on MPO's BuNet site for more information.)

The MPO is responsible for tracking and maintaining documentation reflecting the statuses of all enterprise mobile application requests, reviews, and approval decisions. The MPO must present a ToU agreement to a user prior to the deployment and installation of an approved, or white-listed, custom mobile app, notifying the user of any restrictions established during the request process and of relevant privacy policies.

Procedures must be instituted, maintained, and regularly reviewed by the ESOC, in conjunction with the MPO, for the continuous monitoring of approved, released mobile apps for any security vulnerabilities.

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.

4.3.5.2. Updating Mobile Applications on Enterprise Mobile Devices

Updates to mobile apps may be provided by the MPO at its discretion, but FBI end users will generally be responsible for installing updates not provided by MPO.

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 and without notification 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 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 *Removable Electronic Storage (RES) Media Protection Policy Directive* (0247D).

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

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:

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-Accessible[1]	VPN
Internet Router	Yes	Limited[2,3]	Yes	No
Desktop	No	No	Yes	No
Printer	No	No	No	No
Laptop	No	No[2,3]	Yes	No
Smart Phone	No	No	Yes	No
Tablet/Hybrid	No	No	Yes	No
Audio Only (e.g., Speakers or Headphones)	Yes	Limited[3]	Yes	No
Wearables With Memory[4]	No	No	Yes	No
Wearable Without Memory[5]	Yes	Limited[3]	Yes	No
Vehicle (Power/Charge Only)	Limited[6]	No	N/A	N/A
Vehicle (Voice Only)	Limited[6]	Limited[3,6]	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

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-Accessible[1]	VPN

Notes
1: Web-accessible 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-Accessible[1]	VPN
UNet Desktop	Limited[2,3]	No	Yes	No
UNet Laptop	Yes	Limited[7]	Yes	Limited[10]
Cloud Service APIs[4]	No	No	Yes	No
Cloud Desktop via Remote Desktop Protocols (RDP)[5]	No	No	Yes	Yes

Stand-Alone Desktop[6]	Limited[3]	Limited[7]	Yes	Yes
Smartphone	Limited[3]	Limited[7]	Yes	No
Wearables[8]	Limited[3]	Limited[7]	Yes	No
Tablet[9]	Limited[3]	Limited[7]	Yes	Yes
Stand-Alone[2] Laptop	Limited[3]	Limited[7]	Yes	Yes

Notes

1. Web-accessible 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.
10. Monitoring must be in place when connecting to VPN.

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* (1093PG), 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 the *Security Compliance Program Policy Guide* (0934PG).

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 *Classification Management Policy Guide* (1058PG) 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 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 Life Safety 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 *Self-Reporting Requirements Policy Guide* (1037PG), based on the type of travel. Additionally, for official travel, employees, task force officers (TFO), detailees, and contractors must complete the Beacon Task List prior to travel and must otherwise adhere to the *International Operations Division Policy Guide* (0950PG).

An FBI employee traveling outside of the United States or United States territories on official foreign travel must bring an enterprise mobile device if he or she has been assigned one. Employees traveling to a high- or critical-threat countries must consult with their respective mobility POCs to determine the appropriate device requirements before the foreign travel occurs.

CSOs must ensure that FBI personnel complete foreign travel briefings in accordance with the processes described in *Self-Reporting Requirements Policy Guide* (1037PG) based on the type of travel.

4.3.10.1.1. Cellular Service on Enterprise Mobile Devices

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. FBI personnel traveling to these locations must consult with their respective mobility POCs to ensure this action is performed.

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 maintain positive control over their devices, unless there is a demonstrable security or operational need to deviate from this practice. 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, including voice, SMS text, and MMS during foreign travel. Furthermore, any use that incurs more than a negligible expense to the government must only be for a legitimate business purpose.

When a device is in use but is not connected to a USG-issued or USG-controlled wireless access point, the device must have its Wi-Fi disabled.

For travel to low- or moderate-threat countries:

- 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. When not in use, Wi-Fi must be disabled.
- All wireless communications, including, but not limited to, Bluetooth, NFC, and GPS capabilities, must be disabled at all times.

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.

4.3.10.2.7. Incident Reporting

FBI personnel must follow the procedures described in the *Security Compliance Program Policy Guide* (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 the *Security Compliance Program Policy Guide* (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 *Self-Reporting Requirements Policy Guide* (1037PG), 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 the *Security Compliance Program Policy Guide* (0934PG).

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

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. FBIHQ division and FO heads have the authority to suspend, remove, revoke, and/or reallocate all enterprise mobile devices within their respective divisions and FOs. 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.

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.

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 (with the MPO on the distribution list) for approval. b7E

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 Operations, Safeguarding, and Backstopping Policy Guide* (1000PG).

4.4.2. Section 508

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 the *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 the *External Security Marking of Information Technology Hardware and Electronic Data Storage Media Policy Guide* (0636D).

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).

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 the *Encryption of Electronic FBI Information Policy Directive* (0592D).

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

Mobile applications on enterprise mobile devices are assessed and then approved or rejected through a Mobile Applications Review Process. All approved mobile apps must be added by the MPO to the FBI's white list. Users may only download FBI-approved mobile applications from the managed Google Play Store and/or the FBI's App Catalogue. Blacklisted commercial mobile applications identified by MPO or SecD will not be permitted on enterprise mobile devices. 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.

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.

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.

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 their 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.

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 the *Destruction of Classified and Sensitive Material Policy Directive* (0506D).

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 the *Security Assessment and Authorization for FBI Information Systems Policy Directive* (0655D).

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 [redacted] The FBI authorizing official may only designate authority for b7E

exemption approvals to persons holding Senior Executive Service (SES) or Senior Level (SL) positions or higher.

All enterprise exemptions must be incorporated into this PG.

Individual waivers to the procedures and processes within this PG must be approved by the division head (i.e., SecD or ITID) that has program ownership.

5. 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 2880.1C, *Information Resource Management Program*
- DOJ Order 0902, Accessible Electronic and Information Technology (October 15, 2015)
- DOJ Order 0908, *Use and Monitoring of DOJ Information Technology, Information Systems, and Access to an Authorized Users' Electronic Information* (August 18, 2020)

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.

Appendix A: References

- Assurance Management Unit, OCIO
- MPO, ITID
- Attachment A, *Mobile Device Restrictions Quick Reference Guide (QRG)*
- Attachment B, *Laptops in FBI Sensitive Compartmented Information Facilities Quick Reference Guide (QRG)*
- *Classification 319, Managing the FBI's Administrative Records*
- Committee on National Security Systems Instruction (CNSSI) No. 22, *Policy on Information Assurance Risk Management for National Security Systems*
- CNSSI No. 4009, National Information Assurance (IA) Glossary
- FD-1001, "Consent for Warrantless Searches of Department of Justice Workplaces"
- *Courier Program Policy Directive and Policy Guide* (0719DPG)
- *Digital Evidence Policy Guide* (0830PG)
- DOJ Mobile Device and Mobile Application Security Policy Instruction
- 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*
- EO 13556, *Controlled Unclassified Information*
- FBI Critical and High Threat Country Life Safety List
- *FBI Ethics and Integrity Program Policy Guide* (1120PG)
- *Memorandums of Understanding and Noncontractual Agreements Policy Guide* (1031PG)
- FBI SPL
- *Frequently Asked Questions Regarding Social Media and the Hatch Act*
- *Government Vehicle Use Policy Guide* (1093PG)
- ICD Number 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*
- ICD Number 705, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*
- Information and Technology Branch (ITB) Enterprise Mobility Strategy
- Information Assurance (IA) Policy Compliance Assessment Plan
- Instructions for DOJ IT Resources Outside of U.S. Territory Waiver Request
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision (Rev.) 1, *Guide for Conducting Risk Assessments*

- NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
- *Removable Electronic Storage (RES) Media Protection Policy Directive* (0247D)
- *Destruction of Classified and Sensitive Material Policy Directive* (0506D)
- *Encryption of Electronic FBI Information Policy Directive* (0592D)
- *Security Compliance Program Policy Guide* (0934PG)
- *Security Assessment and Authorization for FBI Information Systems Policy Directive* (0655D)
- *Security Assessment and Authorization Policy Guide* (0655PG)
- *External Security Marking of Information Technology Hardware and Electronic Data Storage Media Policy Directive* (0636D)
- *Federal Bureau of Investigation (FBI) Unclassified Network (UNet) Enclave Policy Directive* (0723D)
- *Non-Retaliation for Reporting Compliance Risks Policy Directive* (0727D)
- *Reporting FBI Employee Misconduct Policy Directive* (0796D)
- *FBI Accessible Information and Communication Technology Policy Directive* (0919D)
- *Self-Reporting Requirements Policy Guide* (1037PG)
- Presidential and Federal Records Act Amendments of 2014
- FD-281, "Receipt for Government Property"
- *Records Management Policy Guide* (0769PG)
- Rehabilitation Act of 1973
- *Remote Access for General and Privileged Users Policy Guide* (0655PG-4)
- *Classification Management Policy Guide* (1058PG)
- Section 508 Program Team
- *Social Media and Other Electronic Information Sharing Technologies Policy Directive and Policy Guide* (0579DPG)
- *Undercover Operations, Safeguarding, and Backstopping Policy Guide* (1000PG)

Appendix B: Definitions and Acronyms

Definitions

Application program interface: 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.

Authorizing official: 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 CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

Black list: a list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity. [Source: CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

Bring your own device: 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.

Cloud resource: 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:

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).
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.

Cloud service: a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable Internet accessible cloud resources.

Covert operation: aee undercover operation.

Enterprise mobile device: an FBI-owned mobile device issued by the MPO that is associated with an enclave FBI information system.

FBI information system: 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 CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

FBI personnel: 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.

FBI-controlled facility: 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.

IT resource: any information system, device, network, or account that processes, stores, or transmits information.

Logical connection: connection of a device to an information system, another device, a network, or an account through a server or network configuration.

Logical HTTPS: 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.

Medical device: a device prescribed for the purposes of maintaining life standards (e.g., hearing aids, pacemakers, implanted medical devices).

Mobile application: 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.

Mobile backend: 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.

Mobile device: a portable computing device that:

- Is physically small and can easily be carried by a single individual.
- Is designed to operate without a physical connection (e.g., wirelessly transmit or receive information).
- Possesses local, nonremovable data storage.
- Is powered-on for extended periods of time with a self-contained power source.

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 CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

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

- The MDM or a successor service
- The MAM or a successor service
- The mBaaS API or a successor service
- Computing, storage, and analytics enabling content provided to end-user devices

Near-field communication: a set of standards for mobile devices to establish radio communication with each other by touching them together or bringing them into close proximity.

Non-FBI-owned mobile device: a mobile device that is OGA (including local, state, and tribal law enforcement)-, contractor-, vendor-, or visitor-owned or is personally owned.

Official foreign travel: travel that is performed at the direction of the FBI and in support of its mission(s) within a foreign country. Travel to Puerto Rico, the U.S. Virgin Islands, Guam, or other U.S. protectorates, possessions, or territories is not considered foreign travel.

OGA-owned mobile device: a government-furnished or local, state, or tribal law enforcement device issued for the purposes of official USG business.

Overt operation: an FBI mission or function that occurs on a normal day-to-day basis.

Personally identifiable information: 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 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.

Product charter: 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.

Proxy: 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.

Reasonable suspicion: 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.

Record: 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.

Red/black separation: 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 CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

Remote desktop protocol: 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.

Resource: a source or supply from which benefit is produced. Typically, resources are materials, energy, services, staff, knowledge, or other assets.

Security monitoring: the practice of monitoring, tracking, logging, analyzing, and responding, 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.

Sensitive Compartmented Information facility: accredited area, room, or group of rooms, buildings, or installation where sensitive compartmented information may be stored, used, discussed, and/or processed. [Source: CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

Signal enhancement device: a device that takes an existing signal from an access point or wireless router and rebroadcasts it to create a second network.

Stand-alone device: a computer resource that is not directly connected to a corporate network, but may be connected to the Internet.

Strong encryption: 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.

System security documentation: 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 CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

TEMPEST: a name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. [Source: CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

Undercover operation: an FBI mission or function that includes [redacted] sensitive operations. b7E

United States government information: 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 CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

Virtual Private Network: 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.

Wearable: 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 generally categorized as an Internet of Things (IoT). Examples include wearable technology, wearable devices, and smart wearable devices.

White list: 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: CNSSI No. 4009, *National Information Assurance (IA) Glossary*]

Wireless connection: 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
AO	authorizing official
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
CD	compact disc

CDC	chief division counsel
CFR	Code of Federal Regulations
CIO	chief information officer
CISO	chief information security officer
CISS	Collaboration and Identity Services Section
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	*Domestic Investigations and Operations Guide*
DOJ	Department of Justice
DPO	division policy officer
DVD	digital versatile disc
EAD	executive assistant director
EC	electronic communication
EISS	Enterprise Information Security Section
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
FD	Finance Division
FISMA	Federal Information Systems Modernization Act
FO	field office
FOS	Field Operations Section
FOUO	For Official Use Only
GPS	Global Positioning System
HIPPA	Health Insurance Portability and Accountability Act
HTTPS	Secure Hypertext Transfer Protocol
IA	information assurance
IaaS	Infrastructure as a Service
IATU	Information Assurance Technology Unit
IC	Intelligence Community
ICD	Intelligence Community Directive
IIS	Internal Investigations Section
INSD	Inspection Division
InTO	Insider Threat Office
IPO	Internal Policy Office
IoT	Internet of Things
ISA	interconnection security agreement
ISP	Internet service provider
ISWS	Information Security Workforce Services [Unit]
IT	information technology

ITB	Information Technology Branch
ITCRMD	Information Technology Customer Relationship and Management Division
ITID	Information Technology Infrastructure Division
ITPfM	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
O365	Microsoft Office 365
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
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
SOS	Security Operations Section
SP	special publication
SPL	Standard Products List
SRS	Strategic Resources Section
SSL	Secure Socket Layer
SSP	system security plan
TCSU	Training Coordination and Support Unit
TD	Training Division
TDY	temporary duty [assignment]
TFO	task force officer
TLS	Transport Layer Security
TODU	Technically Trained Agent Operations and Development Unit
ToU	terms of agreement
TSS	Training Services Section
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

Appendix C: 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			