IT Security Procedural Guide: Securing Mobile Applications and Devices CIO-IT Security-12-67

Revision 7

October 1, 2024

Controlled by: General Services Administration
OCISO ISP Division: ispcompliance@gsa.gov

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – March 27, 2019		
N/A		Initial Release	Mobile Device Security guidance	N/A
		Revision 2		
1	Eaton	Integrated ILS and added additional language	Required revisions	
		Revision 3 – May 20, 2014		
1	Eaton	Made revisions per 2013 audit findings	OIG Audit findings	pp. 4 and 22-24
2	Heard	Made revisions per NIST 800-53, Rev 4	SC-9 incorporated into SC-8 and SC-9 withdrawn	4
3	Heard/Atwater	Verification of links and attachments		Throughout
		Revision 4 – January 26, 2018		
1	Dean/Feliksa	Changes made throughout the document to reflect current procedural guide format	Changes in GSA process and products used to manage mobile devices	Throughout
		Revision 5 – June 16, 2022		
1	IS/ISDT	Primary changes are: ● Updated references and links ● Added Google MDM ● Major revisions to the process sections	Changes in GSA process and products used to manage mobile devices	Throughout
		Revision 6 – April 13, 2023		
1	IS/IDT	Primary changes are: ● Merge and retire Mobile Device Team Standard Operating Procedure ● Added Zscaler ● Added language banning the use of TikTok and ByteDance LTD owned/operated/ associated applications or software. ● Added information on international roaming	Update to new Federal and GSA guidance.	Throughout
2	McCormick/ Klemens	● Updated references and links. ● Updated format to reflect current procedural guide format.	Update to current guide format and style.	Throughout
		Revision 7 – October 1, 2024		
1	Rialti/Normand/ Klemens	Changes included: ● Complete restructuring of guide and renamed to "Securing Mobile Applications and Devices." ● Updated content to reflect current GSA guidance. ● Added NIST controls to be addressed when Mobile apps are included in a System's boundary.	Refocused guide on user responsibilities and restructured accordingly.	Throughout

Approval

IT Security Procedural Guide: Securing Mobile Applications and Devices, CIO-IT Security 12-67, Revision 7, is hereby approved for distribution.

DocuSigned by:

Bo Berlas

FD717926161544E...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

1 Introduction

Mobile applications and devices (i.e., smartphones, tablets), along with the resources they use and/or store, must support the security objectives of confidentiality, integrity, and availability. To achieve these objectives, mobile applications and devices must be secured against a variety of threats. The General Services Administration (GSA) has developed this guide upon the guidance from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124, Revision 2, "Guidelines for Managing the Security of Mobile Devices in the Enterprise."

1.1 Purpose

The purpose of this guide is to establish GSA's procedures and protocols regarding:

- Mobile apps being approved for use
- Mobile device management
- Mobile device usage

This guide also explains the security concerns inherent in mobile device use and provides direction on securing mobile devices throughout their life cycle.

1.2 Scope

1.2.1 Intended Audience

The requirements outlined within this guide apply to, and must be followed by, all GSA Federal employees, contractors, and associates of GSA who acquire, develop, review, and approve mobile applications and/or the types of mobile devices issued as Government Furnished Equipment (GFE).

1.2.2 Mobile Applications

Mobile applications (apps) addressed by this guide include commercial, custom, and other government agency-approved mobile apps developed, deployed, and/or used on GSA-issued GFE.

1.2.3 Mobile Devices

For the purposes of this guide, mobile devices are portable computing devices (i.e., smartphones, tablets). Laptops are specifically excluded from the scope of the guide since the security controls available for laptops are quite different from those available for smartphones and tablets. Mobile devices with minimal computing capability, such as basic cell phones, are also out of scope because of the limited security options available and the limited threats they face.

1.3 Mobile Device Security Overview

Securing Mobile Devices are covered in GSA Order CIO 2100.1, "GSA Information Technology (IT) Policy" as stated in the following paragraphs.

Chapter 2, Section 2; and, Chapter 2, Section 21, Paragraph (f):

"Authorized Users of IT Resources. Authorized users of GSA IT resources, including all Federal employees and contractors, either by direct or indirect connections, are responsible for complying with GSA's IT Security Policy and procedures. Their responsibilities include:

f. Ensuring any sensitive data (e.g., PII, PCI, CUI, authenticators, business sensitive data) stored on any workstations or mobile devices including, but not limited to, laptop computers, notebook computers, external hard drives, USB drives, CD-ROMs/DVDs, and personal digital assistants, are encrypted with GSA-provided encryption."

Chapter 4, Section 1; Paragraph (g), Bullet 8, Sub-bullet (d):

"For password-based authentication:

(d) Passwords for all mobile devices such as GSA approved phones, iPads, and tablets must be a minimum of 6 characters."

Chapter 4, Section 1, Paragraph (gg):

"All GSA workstations and mobile devices shall initiate a device lock after 15 minutes of inactivity. The device lock shall remain in effect until the user re-establishes access using appropriate identification and authentication."

Chapter 4, Section 1, Paragraph (hh), Bullets (1) and (2):

"OAuth 2.0 is an industry standard protocol approved by GSA. It enables a gsa.gov user to grant access to their account or data in Google Apps to a relying party. It is used in a wide variety of services for user authentication. The following policies apply to the use of OAuth 2.0:

(1) GSA IT's OCISO shall monitor and restrict the integration of gsa.gov accounts with OAuth 2.0 to third-party services including but not limited to; websites, Software as a Service (SaaS), mobile applications, and Google Apps Scripts.

(2) Use of the Auth 2.0 Access Scopes listed below is prohibited unless integrated with websites, mobile apps, and SaaS authorized to operate by GSA and/or included in the GSA IT Standards Profile."

Chapter 4, Section 1; Paragraph (hh), Bullet 2, Sub-bullet (f):

"Manage Devices. Administrator's scope to view and manage mobile devices' metadata."

Chapter 4, Section 1; Paragraph (oo):

"All GFE/GSA procured workstations/mobile devices such as phones and tablets, should connect to the GSA Wireless Network which requires an ENT account to access, rather than the Guest Wireless Network. Connecting in this manner will provide access to GSA resources as well as the Internet, similar to the GSA Wired Network."

Chapter 4, Section 3; Paragraph (r):

"GFE must not be taken on international travel without prior approval. Users must submit a GSA IT Service Desk ticket and receive approval from GSA IT and their supervisor with a recommendation for approval or disapproval from the OMA Threat Management Office related to country specific threat assessment.

Covered Individuals, as defined in Security Executive Agency Directive (SEAD) 3, must contact OMA prior to any international travel.

OMA will provide direction on foreign contact, security precautions, mobile devices, etc."

Chapter 4, Section 7; Paragraph (q):

"GSA CIO-IT Security-12-67 provides GSA's specific information security requirements regarding mobile devices and applications. Per CIO-IT Security-12-67, mobile devices include

smartphones and tablets and excludes laptops and basic cell phones. In accordance with CIO-IT Security-12-67:

All mobile applications must follow the approval process described in the guide before being added to any mobile device or being included in a system's boundary.

GSA's Mobile Device Management (MDM) solution must be installed, operating, and managed by GSA on all mobile devices before they connect to any GSA resources.

All mobile applications and devices must be part of a system ATO, or in the case of stand alone applications, receive its own ATO."

Chapter 5, Section 3; Paragraph (c)

"GSA organizations must define procedures to periodically monitor mobile device security to verify compliance with GSA requirements in GSA CIO-IT Security-12-66 and GSA CIO-IT Security-12-67."

Chapter 5, Section 3; Paragraph (l)

"GSA monitors mobile devices using MDM policies and rules of behavior as outlined in GSA CIO-IT Security-12-67."

2 Roles and Responsibilities

The roles and responsibilities provided in this section have been extracted or paraphrased from GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," or summarized from GSA and Federal guidance. The responsibilities listed in this guide are specific to mobile application and device security, a complete set of GSA security roles and responsibilities can be found in CIO 2100.1.

2.1 Chief Information Security Officer (CISO)

The GSA CISO is responsible for overseeing the development, publishing, and effectiveness of this IT security guide addressing the security of mobile applications and devices in accordance with Federal laws, regulations, and guidance. The CISO coordinates with the OCISO Division Directors, the Mobile Device Management Team, and others within GSA to establish the procedures for securing mobile applications and devices throughout their life cycles. The CISO concurs on authorization to operate (ATO) letters for mobile applications and devices, standalone, or as part of another GSA system.

2.2 Office of the Chief Technology Officer (OCTO)

The OCTO has responsibility for maintaining the authoritative list of IT Standards and approved technologies, as well as associated metadata, currently maintained at the GSA Enterprise Architecture Analytics and Reporting (GEAR) website. The OCTO is also responsible for reviewing business use cases for mobile applications to ensure they comply with GSA's requirements.

2.3 Authorizing Official (AO)

The AO is responsible for:

- Ensuring an acceptable level of risk for a system is achieved based on the security and privacy controls implemented for a system or inherited from another system
- Authorizing the operation GSA systems under their purview, including mobile applications and devices, as applicable

2.4 System Owner

The System Owner is responsible for ensuring:

- Systems and the data they process have necessary security and privacy controls in place and are operating as intended
- An ATO is issued for systems under their purview prior to being placed into production, including systems with mobile applications and devices, as applicable
- Security is maintained throughout the lifecycle of their systems

2.5 Mobile Device Team

The Mobile Device Team is responsible for:

- Managing the configuration of mobile devices and restrictions on the usage of mobile devices and applications
- Monitoring mobile devices using GSA's Mobile Device Management (MDM) capability and acting when devices are non-compliant with GSA's security and privacy requirements.
- Coordinating with the OCISO on security technologies installed and used on mobile devices, and on requests for applications to be allowed on devices.
- Collaborating on the acquisition of mobile devices and applications used for MDM.

2.6 Mobile Device Users

Mobile device users are responsible for using and securing their mobile devices as specified in:

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Policy"
- GSA Order CIO 2104.1, "GSA Information Technology (IT) General Rules of Behavior"
- GSA's Mobile Devices InSite webpage

Additional user responsibilities are:

- A user may not connect a mobile device to GSA resources (Mail, Drive, etc.) or store any GSA data on any GFE without complying with all aspects of this guide.
- Both Android and iOS (Apple devices) have certain user-controlled functions that must also be adhered to at all times. The following are mandatory settings and must be set by the user and not changed/removed at any time.

  For Android devices:

  - All devices must have the GSA's Enterprise Mobility Management (EMM) apps loaded and kept up to date.
  - Unknown Sources must remain unchecked in the device settings.
  - Auto-update of apps must be enabled (this also ensures all non-security related apps

are kept updated for user benefit)

For iOS (Apple) devices:

- All devices must have the GSA's EMM apps loaded and kept up to date.
- Unknown Sources must remain unchecked in the device settings.
- Auto-update of apps must be enabled (this also ensures all non-security related apps are kept updated for user benefit)
- All apps must be kept up to date from the "App Store" icon. **Note**: A small red number will appear next to the icon when an app requires updating.

Note: User compliance is mandatory and deviation from the requirements specified above constitute a violation of GSA policy and shall be addressed by Administrators or IT Security personnel as outlined below, depending on the actual non-compliant event and its seriousness. Recurring violations of compliance standards are grounds to potentially remove access to GSA resources without prior notification. These compliance enforcement steps are taken in the order listed below and are enforced, based on the situation and severity of the issue:

- Contacting the user to notify them of non-compliance and rectifying actions required.
- Blocking the user's access to GSA resources via GSA's MDM solutions.
- Locking the user's device remotely, forcing the user to contact the IT Service Desk to correct the non-compliant event.
- Remotely wiping the device, whether it be a selective (GSA data only) or full wipe.

3 Mobile Device Security Procedures and Requirements

3.1 Mobile Device Solution Lifecycle

NIST SP 800-124 outlines how the concepts presented in this guide should be incorporated throughout the entire life cycle of enterprise mobile device solutions, involving everything from policy to operations. The section references a five-phase life cycle model to help outline at what point in their mobile device solution deployments a recommendation may be relevant. Per NIST SP 800-124, the steps of an Enterprise Mobile Device Deployment Lifecycle are as listed below. Following each step is a brief description of how GSA implements each step.

- **Step 1 - Identify Mobile Device Requirements:** GSA's current mobile device requirements are provided at the GSA Mobile Support Site with additional security requirements documented within this guide.
- **Step 2 - Perform Risk Assessment:** Risk assessments are performed for devices as described in Section 3.2 and for mobile applications in Section 4.3.1.
- **Step 3 - Implement Enterprise Mobility Strategy:** GSA's mobility strategy is summarized in Section 4, with additional details throughout this guide and the GSA Mobile Support Site.
- **Step 4 - Operate & Maintain:** GSA operates and maintains mobile GFE as specified throughout this guide and the GSA Mobile Support Site.
- **Step 5 - Dispose and/or Reuse Devices:** GSA's Mobile Device Team's internal processes for mobile devices include steps to take when reissuing or disposing of devices (e.g., wiping devices and internal storage, resetting).

3.2 GFE Mobile Devices

All GFE mobile devices (i.e., smartphones and tablets) must be acquired in accordance with the

Procurement of Mobile Devices webpage. From a Cyber-Supply Chain Risk Management (C-SCRM) perspective, GSAM 504.70 identifies acquisition requirements and CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program describes pre-award, post-award, and ongoing (monitoring) C-SCRM activities and support. OCIO will manage and provide technical support for smartphones and tablet devices. Service and/or Staff Offices (S/SO) may purchase subject devices, in accordance with applicable law and regulations, when it has been determined that a business need can support such a purchase. It is imperative that all aspects of the Federal Acquisition Regulation (FAR) be followed when purchasing mobile devices, including brand name justification requirements.

All smartphone and tablet types must be on the GSA Approved Devices list prior to use at GSA. The Mobile Team coordinates with OCISO, and others as applicable, when new devices or technologies are acquired or integrated into devices. This assessment, once completed, constitutes approval for as long as devices of these types are in use throughout the enterprise.

GSA has outlined, for users and administrators, all approved devices (government and personally procured), the hardening requirements for each, as well as all policies and programs for users & administrators can be found on the GSA Mobile Support Site.

Found on the site are:

- A listing of all approved devices – these devices are tested by the Mobile Device team and certified/approved by the OCIO, ISSM before release to users End of Life Devices
- Mobile Device/Application policies
- Use of the “Application Specific Password”
- An outline of policy for procurement of government mobile devices

This site is maintained by the Mobile Device Team under the supervision of the Director of Infrastructure Solutions Division (IDTS), OCIO, and the GSA Infrastructure ISSM who is charged with overall management of GSA’s mobile device security strategy.

3.2.1 Mobile Device Remote Administration

Remote control by the Mobile Team of GSA mobile devices may be authorized when:

- The location of a GSA user or GFE mobile device is unknown.
- A GSA user is suspended, terminated, charged, or arrested for any type of misconduct or malfeasance.

In such cases the mobile device may be remotely controlled to:

- Locate the individual or device
- Protect (e.g., lock) or wipe the GFE mobile device and data.

3.2.2 Notification and Reporting

The monitoring tools used by GSA notify/alert the Mobile Device Team, OCISO personnel, and the user when triggers identify an issue, anomaly, or flaw. The personnel notified are responsible for reporting and escalating issues/incidents in accordance with CIO-IT Security-01-02: Incident Response (IR). Flaws/vulnerabilities must be resolved and reported per CIO-IT Security-06-30 regarding NIST SP 800-53, Revision 5, control RA-05, Vulnerability Monitoring and Scanning.

4 Enterprise Mobility Management (EMM)

The GSA EMM Strategy aligns to NIST SP 800-124 for Enterprise Mobility Management. EMM, which is sometimes referred to as UEM (unified endpoint management), is a solution used to deploy, configure, and actively manage mobile devices in an enterprise environment. GSAs EMM includes management technologies for Mobile Device Management (MDM), Mobile Threat Detection (MTD), and Mobile Application Management (MAM) as defined below:

4.1 Mobile Device Management (MDM)

GSA has enterprise MDM technologies for the management, configuration control, and administration of its iOS, iPadOS, and Android devices. GSA utilizes MaaS360, a FedRAMP-authorized cloud SaaS for iOS and IpadOS and Google MDM for Android Devices. GSA's MDM solutions help GSA to protects its data and optimize GSA mobile devices for productivity, enabling employees to work anytime and anywhere through trusted mobile interactions. GSA's MDM solutions allow GSA to activate and configure devices over the air for instant set-up; monitor and control the security posture of smartphones and tablets; distribute, secure and manage mobile apps; and, enforce policy compliance for stronger data protection. GSA's defense in depth implementation of its MDM technologies ensures:

- Policy violations are automatically identified and reported.
- Enables strong encryption of data communications between the mobile device and the organization.
- Remotely wipes mobile devices (to scrub its stored data) if it is suspected that the device has been lost, stolen, or otherwise fallen into untrusted hands.
- Requires a password/passcode and/or other authentication (e.g., domain authentication) before accessing the organization's resources. This includes basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out the account, wiping the device). All managed devices have a passcode with a minimum of a 6-character passcode.
- MDM as well as device configuration policies ensure that the device automatically locks itself after it is idle for a period.
- If device account lockout is enabled or the device password/passcode is forgotten, an administrator can reset this remotely to restore access to the device using MDM in addition to device configuration policies.
- Has established device configuration policies to ensure a device automatically locks itself after it is idle for a specified period.
- Manages installs, updates, and removal of applications.
- Limits and prevents access to the enterprise based on the mobile device's status (e.g., up-to-date versions of software, including OS, device not jailbroken/rooted).
- Does not restrict user and application access to GFE mobile device's digital camera, GPS, and Bluetooth interface.
- Restricts data from being accessed via the USB interface, to include removable storage. Users may request a waiver to this restriction based on a valid business operational need.

The MDM Policies 9/30/2024 Google folder contains the following configuration setting files:

- GSA_DEP_UNASSIGNED_ACTIVE
- GSA_MDM_DEP_ZCC (6)

- GSA_MDM_DEP_ZCC_NNM
- Non_Compliant_OS_-_Stage_2 (2)
- USB_Exception_-_GSA_MDM_DEP_ZCC_NNM

4.2 Mobile Threat Defense (MTD)

MTDs are a set of technologies that protect mobile devices from threats. MTDs can detect known and unknown threats by analyzing a device's behavior and traffic. It can identify applications that behave like malware, anomalous network traffic, and advanced phishing attacks. GSA employs solutions that protect mobile devices from malicious activities during the device's use. The mobile security technologies currently deployed for this purpose are:

- Mobile Endpoint Detection and Response (EDR): GSA's implementation of Lookout for Work identifies potential threats on its mobile devices. Lookout for Work is deployed across GSA mobile devices to protects from threats and compliance violations with enterprise corporate policies. When a threat has been detected, Lookout provides employees and administrators remediation options (e.g., uninstall app, invoke conditional access).
- Secure Access Secure Edge (SASE): GSAs implementation of zScaler Internet Access (ZIA) provides web, firewall, and domain name system (DNS) functionality for all outbound connections. All GFE mobile traffic is centrally routed through ZIA to ensure GSA security and access policies are enforced when accessing the Internet.

4.3 Mobile Application Management (MAM)

Mobile applications available on Apple App and Google Play stores are broadly available to GSA associates and contractors for download. Mobile Applications on the GSA Banned Mobile Apps list as identified in the Mobile Support Site are prohibited and security controlled. To improve its mobile security posture, GSA is transitioning to a comprehensive Allow List policy that aligns with its Zero Trust Strategy - only apps on the approved list will be available for download and use on government-issued devices.

The mobile app Allow list will be managed as part of GSA's IT Standards List.

4.3.1 Mobile Application Allow List

When a GSA employee identifies an app they want to use and it is not currently listed as approved on the IT Standards List, the user must complete and submit a Mobile App Allowlist Request in ServiceNow. The Requestor must complete all of the required information within the ServiceNow request and submit it.

Mobile applications are subject to review by the GSA IT Security team at any time. Mobile applications may be re-categorized into one of the above categories based on such a review.

Once the app is categorized and an assessment completed and/or approval received, the status is noted and the app is added to the IT Standards List. Mobile apps are categorized as:

Approved:

- GSA (or other Federal Agency) apps that have undergone an assessment and authorization process and received an ATO as outlined in CIO-IT Security 06-30: Managing Enterprise Cybersecurity Risk, and are published in either the Apple iTunes or Google Play store, or

- Apps on the GSA Approved List will be available for download and use on government-issued devices. Users may submit a mobile application request for GSA IT Security team review and approval consideration for inclusion in the GSA Approved List. Reference Appendix A.

Not Approved: Apps that have undergone a GSA IT Security team review and were deemed unacceptable based on any/all of the criteria in Appendix A.

4.3.2 Mobile Application Review and Approval Process

The following steps describe the process when a mobile app is approved at every step in the process.

1. A user submits a Mobile App Allowlist Request.
2. Their supervisor approves the request.
3. An ISO Endpoint Management review is initiated, after the review is completed and the app is approved, for:
   a. **Integrated Mobile Apps**: If the app is used in support of a GSA information system it must be added to the system's SSPP and added to its assessed boundary. See Appendix B for additional details on required updates.
   b. **Standalone Mobile Apps**: If the app is standalone, it undergoes an Enterprise Application and Infrastructure Security Team (ISTE) Criteria Review. See Appendix A for additional details.
4. Upon security approval, the GSA OCTO will review the business case justification for the usage of the mobile app to ensure it complies with GSA's requirements. Upon approval CTO will add the app to the IT Standards List as part of the Mobile App Allow List.
5. GSA MDM tooling will be used to manage the deployment of allowed/approved Mobile apps to GFE devices. Once on the allowed list users are able to install and use the approved mobile app.

Note: At any step in the process a request may be rejected, and the process ends at that any point.

4.3.3 Updates to Mobile Apps

The Mobile Device Team makes updates to apps available once they have been approved. For devices with the app already installed the update is pushed to the device. For devices without the app installed, the updated app is made available through GSA's approved platform stores for devices to download.

4.3.4 Removal of Mobile Apps

A mobile app may be removed immediately by the Mobile Team from the GSA Mobile Application Allowed List and GFE devices if a security, operational, or compliance vulnerability has been identified.

A mobile app may also be removed when an AO, or their designee, notifies the Mobile Device Team that the app is no longer authorized.

5 GSA App Development, Assessment, Authorization, and Deployment

GSA-developed custom applications, in support of business line functions, follow the process outlined below for Android and iOS (Apple) deployments:

- The developer must coordinate with the system team to coordinate development of the app (i.e., development environment, development and user testing, etc.).
- Mobile app scanning throughout development is critical to successful deployment of an app. Before being approved for use, a mobile app must be scanned by the OCISO Security Operations (ISO) Division using an approved scanner.
- All mobile application development must use the Open Web Application Security Project (OWASP) Mobile Security Project in developing mobile apps for guidance during development and testing of an app.
    - OWASP Mobile Application Security Project
    - OWASP Mobile Application Security Testing Guide

5.1 Assessment and Authorization

GSA-developed apps are designed to allow users to access GSA data while mobile. Thus, as GSA business lines develop apps for use on the iOS and Android platforms, these apps must undergo an assessment and authorization process before being deployed. With that in mind, the following guidelines must be followed:

- Apps supporting a GSA FISMA system must be documented in the SSPP (see Appendix B for details) before deployment per CIO-IT Security-06-30. Any app not directly tied to an existing system's ATO must have an assessment performed and subsequently approved for use by the AO.
- Any mobile app development should result in a release of both an iOS and Android version of the app. This ensures coverage to all users within GSA and the maximum coverage for any apps released to the public.
- As with all applications in use by GSA:
    - No High or Critical findings are allowed from the app's scan results. Such findings must be resolved, and a new scan executed showing no High or Critical findings before deployment.
    - Moderate and Low findings must be documented in Plan of Action and Milestones (POA&Ms) for the system by which the app is authorized.

Note: Additional information on POA&M requirements and timelines can be found in CIO-IT Security-06-30 and CIO-IT Security-09-44: Plan of Action and Milestones (POA&M).

5.2 Privacy

Privacy considerations must be addressed for both COTS and GSA-developed apps and adhere to the following guidelines:

Each mobile app must have a Privacy Threshold Assessment (PTA) completed by the app developer or sponsor, to determine if the app collects, stores, processes, or transmits PII. PTA's are completed in GSA's Governance, Risk and Compliance (GRC) tool which initiates a review by the Privacy Office.

If the app collects, stores, processes, or transmits PII or other sensitive GSA data, a Privacy Impact Assessment (PIA) must be generated for the app and filed for consideration by the GSA Privacy Office. If the GSA Privacy Office determines that a Statement of Records Notice (SORN) is also required, the app developer or sponsor must draft it as well.

Apps requiring a PIA must be authorized at the FIPS 199 PUB Moderate level. A Privacy Act Statement (i.e., Privacy Notice) or Privacy Notice, as applicable must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement or Notice must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement or Notice from the form is acceptable.

Note: Apps that access data a user creates must assume a user may include privacy data/PII in the application unless the data creation is restricted to data controlled by the app.

Examples of Privacy Act Statements for mobile apps are provided below:

Example Privacy Notice (No PII): This mobile application does not collect your personal information. We collect only [developer insert information here].

Example Privacy Notice (with PII): This mobile application collects your personal information. We collect [developer insert information here]. Your personal information is collected so we can [developer insert information here]. Your personal information is stored in [developer insert information here] GSA system. For additional information, please visit GSA’s [insert appropriate SORN] and [insert appropriate PIA] for this app.

Appendix A. Mobile App Use Cases

Mobile apps are evaluated based on the following use cases and are approved or rejected for use based on the results of the process/action identified.

Table A-1. Mobile App Use Cases

Use Case	Accept/Reject Process
Mobile Apps required for work having a legitimate business case but is not on the approved list?	**Approve/Reject** for use based on ISTE mobile app testing.
The Mobile app stores data on a GFE and does not transmit the data to the vendor's Cloud ecosystem.	**Approve/Reject** for use based on ISTE mobile app testing.
The Mobile app directly stores and feeds data to a FedRAMP authorized CSP AND is authorized to operate at the GSA (e.g., Google).	**Approve/Reject** for use based on ISTE mobile app testing. Must be able to support IS guidelines for MFA, encryption, etc.
The Mobile app stores and feeds data to a FedRAMP authorized Cloud Service Provider (CSP) that is NOT authorized for use at GSA.	**Reject**. **Action:** Facilitate CISO/Director meeting for extenuating circumstances (e.g., used to access another agency's CSP for collaboration).
The Mobile app directly stores and feeds data to a CSP that is NOT FedRAMP authorized.	**Reject**. **Action:** Facilitate a meeting between stakeholders to gauge interest in FedRAMP sponsorship.

Appendix B. SSPP Requirements for Mobile Apps

When a mobile app is integrated with an information system, the FISMA System Owner and the system ISSO must review the following sections of the system's SSPP and make the required updates before the mobile app can be deployed within the system's production environment. The system's ISSM must verify the SSPP updates have been completed.

1. Update the SSPP to add the integration of the mobile app with the system as part of the System Description; **Section 9, General System Description.** This section must include how the mobile app is used within the system and, if applicable, describe any new service or function based on its use.
2. **Section 10.3, Software Inventory.** Include the Mobile app in the software inventory.
3. **Section 10.4, Data Flow (and Figure 10-1).** Include any data flows associated with the mobile app and its use.
4. **Section 10.6, Ports, Protocols, and Services (and Table 10-4)**. Include any new ports/protocols/services used by the mobile app, if any. If an existing port, protocol, or service is used, add the app use in the purpose statement.
5. **NIST SP 800-53 Security Controls.** The security controls listed in Table B-1 are to include information about the mobile app, when mobile app-specific actions, attribution, or interaction can be ascertained.

NOTE: Under current NIST and GSA guidance, the controls listed below are only applicable at the Federal Information Processing Standards Publication (FIPS) Pub 199, "Standards for Security Categorization of Federal Information and Information Systems" levels indicated within the FIPS Levels column (L-Low, M-Moderate, H-High).

In the cases of a mobile app integrating into a FIPS Low system where the control is not applicable, the affected Low system is required to include the control, but only as it pertains to the mobile app.

Table B-1 presents NIST SP 800-53 controls required to be updated if:

- There are separate control features for the mobile app being integrated with the system
- The mobile app changes how the system implements a control

If the mobile app relies on the system for control implementation and there is no change to how the controls are implemented then they don't need to address them. Controls may be inherited from other systems, if applicable.

Note: Controls highlighted in purple in Table B-1 are required for systems with Personally Identifiable Information.

Table B-1. Requirements for NIST Control Implementation

NIST Control	FIPS Levels	Instructions for Control Implementation
AC-02: Account Management	L, M, H	If accounts are managed differently for users using the mobile app, revise to include how they are managed.
AC-03: Access Enforcement	L, M, H	If access enforcement is managed differently for the mobile app, revise to include how it is managed.
AC-03(14): Access Enforcement | Individual Access	M, H	If mechanisms providing a user access to their PII is different for the mobile app, revise to include how it is managed.
AC-04: Information Flow Enforcement	M, H	If information flow is enforced differently for the mobile app, revise to include how it is enforced.
AC-06: Least Privilege	M, H	If least privilege is implemented differently for the mobile app, revise to include how it is implemented.
AC-08: System Use Notification	L, M, H	If the system use notification is implemented differently for the mobile app, revise to include how it is implemented.
AC-11: Device Lock	M, H	Revise to include how device locking is implemented for the mobile app.
AC-11(01): Device Lock | Pattern-Hiding Displays	M, H	Revise to include how information on device display is hidden.
AC-12: Session Termination	M, H	If session termination is implemented differently for the mobile app, revise to include how it is implemented.
AC-19: Access Control for Mobile Devices	L, M, H	Revise to include: ● the implementation of requirements on configuration and connection ● guidance on the use of the mobile app, including use outside of controlled areas, and ● the authorization of the mobile app's use.
AC-19(05): Access Control for Mobile Devices | Full Device or Container-Based Encryption	M, H	Revise to include how full device or container-based encryption is implemented on mobile devices.
AU-02: Event Logging	L, M, H	Revise to include how the mobile app implements event logging to meet the control requirements.
AU-03: Content of Audit Records	L, M, H	If audit record contents are different for the mobile app, revise to include the contents of its records.
AU-03(03): Content of Audit Records | Limit Personally Identifiable Information Elements	M, H	If limiting PII in audit records is implemented differently for the mobile app, revise to include how it is implemented.
AU-12: Audit Record Generation	L, M, H	If audit record generation is implemented differently for the mobile app, revise to include how it is implemented.
CA-08: Penetration Testing	L, M, H	If penetration testing is conducted differently for the mobile app, revise to include how it is conducted.
CM-02: Baseline Configuration	L, M, H	If baseline configuration is implemented differently for the mobile app, revise to include how it is implemented.
CM-07: Least Functionality	L, M, H	If least functionality is implemented differently for the mobile app, revise to include how it is implemented.
IA-02: Identification and Authentication (Organizational Users)	L, M, H	If identifiers or authentication is implemented differently within the mobile app, describe how they are implemented.

NIST Control	FIPS Levels	Instructions for Control Implementation
IA-02(01): Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Privileged Accounts	L, M, H	If MFA is implemented differently within the mobile app for privileged users, describe how it is implemented.
IA-02(02): Identification and Authentication (Organizational Users) | Multi-Factor Authentication to Non-Privileged Accounts	L, M, H	If MFA is implemented differently within the mobile app for non-privileged users, describe how it is implemented.
IA-02(05): Identification and Authentication (Organizational Users) | Individual Authentication With Group Authentication	H	If shared accounts or authenticators are implemented differently within the mobile app, describe how they are implemented.
IA-02(08): Identification and Authentication (Organizational Users) | Access to Accounts - Replay Resistant	L, M, H	If replay resistant authentication is implemented differently within the mobile app, describe how it is implemented.
IA-03: Device Identification and Authentication	M, H	Revise the control implementation to identify how device identification and authentication is implemented for the Mobile app, if applicable.
IA-05: Authenticator Management	L, M, H	If authenticator management is implemented differently within the mobile app, describe how it is implemented.
IA-06: Authenticator Feedback	L, M, H	If authenticator feedback is implemented differently within the mobile app, describe how it is implemented.
IA-07: Cryptographic Module Authentication	L, M, H	If cryptographic module authentication is implemented differently within the mobile app, describe how it is implemented.
IA-08: Identification and Authentication (Non-Organizational Users)	L, M, H	If authentication and authentication of non-organizational users (or processes acting on their behalf) is implemented differently within the mobile app, describe how it is implemented.
IA-12: Identity Proofing	M, H	If identity proofing is implemented differently for the mobile app, describe how it is implemented.
IR-02(03): Incident Response Training | Breach	H	If incident response training regarding PII breaches is implemented differently for the mobile app, describe how it is implemented.
IR-08(01): Incident Response Plan | Breaches	M, H	If the incident response plan regarding PII breaches is implemented differently for the mobile app, describe how it is implemented.
MP-06: Media Sanitization	L, M, H	Revise to include how media sanitization of mobile devices with the mobile app is implemented.
PL-02: System Security and Privacy Plans	L, M, H	Revise the system's SSPP to address areas and controls as specified within this appendix.
PL-08: Security and Privacy Architectures	L, M, H	Revise to include the mobile app as a part of the security and privacy architecture.
PT-02: Authority to Process Personally Identifiable Information	M, H	If the authority to process PII is different for the mobile app, describe the authority.
PT-03: Personally Identifiable Information Processing Purposes	M, H	If the purposes for processing PII are different for the mobile app, describe the purposes.

NIST Control	FIPS Levels	Instructions for Control Implementation
PT-04: Consent	M, H	If the users' consent to process PII is different for the mobile app, describe the consent.
PT-05: Privacy Notice	M, H	If the Privacy Notice presented to users is different for the mobile app, describe how it is implemented.
PT-05(02): Privacy Notice | Privacy Act Statements	M, H	If the Privacy Act Statements on forms is implemented differently for the mobile app, describe how it is implemented.
PT-06: System of Records Notice	M, H	If the System of Records Notice (SORN) is implemented differently for the mobile app, describe how it is implemented.
PT-06(01): System of Records Notice | Routine Uses	M, H	If the routine uses published in the SORN are implemented differently for the mobile app, describe how they are implemented.
PT-06(02): System of Records Notice | Exemption Rules	M, H	If Privacy Act exemptions claimed are different for the mobile app, describe how they are implemented.
PT-07: Specific Categories of Personally Identifiable Information	M, H	If the encryption used for specific categories of PII are different for the mobile app, describe how it is implemented.
PT-07(01): Specific Categories of Personally Identifiable Information | Social Security Numbers	M, H	If the mobile app processes Social Security numbers differently, describe how they are implemented.
PT-07(02): Specific Categories of Personally Identifiable Information | First Amendment Information	M, H	If the processing of information regarding First Amendment rights is different for the mobile app, describe how it is implemented.
PT-08: Computer Matching Requirements	M, H	If computer matching requirements are different for the mobile app, describe how they are implemented.
RA-08: Privacy Impact Assessments	L, M, H	If the Privacy Threshold Assessment/Privacy Impact Assessment is different for the mobile app, revise to include how they are implemented.
SA-05: System Documentation	L, M, H	If system documentation for the mobile app is implemented differently, describe how it is implemented.
SA-08(33): Security and Privacy Engineering Principles | Minimization	M, H	If the privacy principle of minimization is different for the mobile app, revise to include how it is implemented.
SA-11: Developer Testing and Evaluation	M, H	If developer testing and evaluation is different for mobile apps, revise to include how it is implemented.
SC-07(24): Boundary Protection | Personally Identifiable Information	M, H	If the boundary protection for PII is different for the mobile app, revise to include how it is implemented.
SC-08: Transmission Confidentiality and Integrity	M, H	If protection of transmitted data is different for the mobile app, revise to include how it is protected.
SC-08(01): Transmission Confidentiality and Integrity | Cryptographic Protection	L, M, H	If the cryptographic protection used during transmission is different for the mobile app, revise to include how it is implemented.
SC-13: Cryptographic Protection	L, M, H	If cryptographic protection is implemented differently for the mobile app, revise to include how it is implemented.
SC-17: Public Key Infrastructure Certificates	M, H	If public key certificates are implemented differently for the mobile app, revise to include how they are implemented.

NIST Control	FIPS Levels	Instructions for Control Implementation
SC-28: Protection of Information at Rest	M, H	If the Mobile app stores GSA information, update the implementation details to describe how the information is protected.
SC-28(01): Protection of Information at Rest | Cryptographic Protection	L, M, H	If the Mobile app stores GSA information, update the implementation details to describe the cryptographic protection provided for that information.
SI-12(01): Information Management and Retention | Limit Personally Identifiable Information Elements	M, H	If there is a difference regarding limiting the PII for the mobile app, revise to include how it is implemented.
SI-12(02): Information Management and Retention | Minimize Personally Identifiable Information in Testing, Training, and Research	M, H	If there is a difference in techniques used to minimize the use of PII research, testing, or training for the mobile app, describe how it is implemented.
SI-18: Personally Identifiable Information Quality Operations	M, H	If the implementation of PII quality operations is different for the mobile app, revise to include it is implemented.
SI-18(04): Personally Identifiable Information Quality Operations | Individual Requests	M, H	If mechanisms for correcting or deleting PII are different for the mobile app, revise to include how PII is corrected or deleted.
SI-19: De-identification	M, H	If mechanisms for removing elements of PII are different for the mobile app, revise to include how it is implemented.