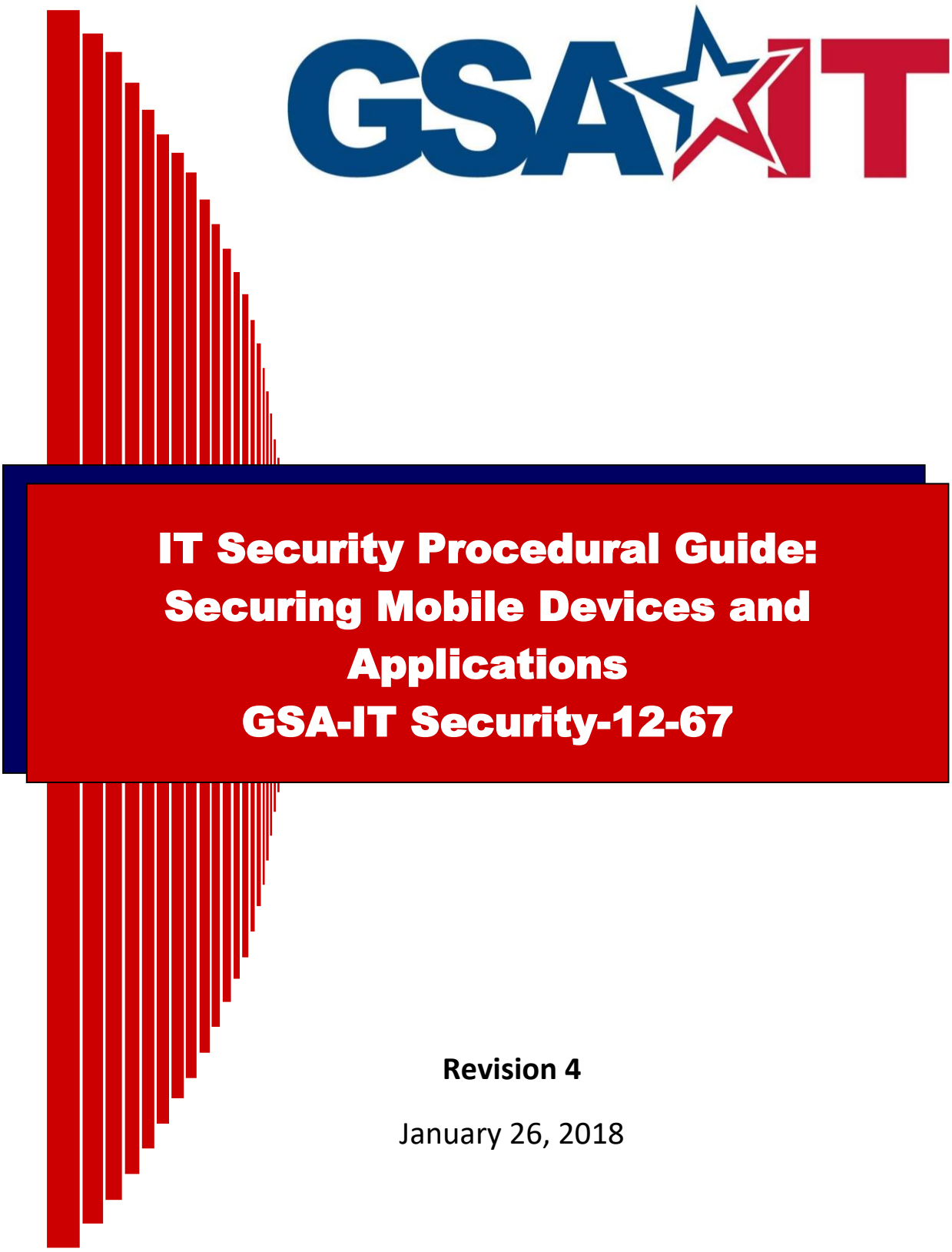

IT Security Procedural Guide: Securing Mobile Devices and Applications GSA-IT Security-12-67

Revision 4

January 26, 2018

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				
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 - 2013	Pages 4 and 22-24
2	Heard	Made revisions per 800 53, Rev 4	SC-9 has been incorporated into SC-8 800 53 rev 4. SC-9 was withdrawn	4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		Throughout

APPROVAL

IT Security Procedural Guide: Securing Mobile Devices and Applications, CIO-IT Security-12-67, Revision 4, is hereby approved for distribution.

1/26/2018

X Kurt Garbars

Kurt Garbars
GSA Chief Information Security Officer
Signed by: KURT GARBARS

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

Table of Contents

Table of Figures

1 Introduction

Mobile devices, like all enterprise devices, need to support the security objectives of confidentiality, integrity, and availability. To achieve these objectives, mobile devices should be secured against a variety of threats. General security recommendations for any IT technology are provided in the latest revision of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*." Specific recommendations for securing mobile devices are presented in this publication and are intended to supplement the controls specified in NIST SP 800-53. Additional specific guidance on mobile devices and applications can be found in the current NIST SP 800-124, Revision 1, "*Guidelines for Managing the Security of Mobile Devices in the Enterprise.*" This guide is built upon the framework outlined in each.

NIST SP 800-124 provides recommendations for securing particular types of mobile devices, such as smart phones and tablets. Laptops are specifically excluded from the scope of the NIST publication and this guide because the security controls available for laptops today are quite different from those available for smartphones, tablets, and other mobile device types. 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.

Centralized mobile device management (MDM) technologies are a growing solution for controlling the use of both organization-issued and personally-owned mobile devices by enterprise users. In addition to managing the configuration and security of mobile devices, these technologies offer other features, such as providing secure access to enterprise computing resources. There are two basic approaches to centralized mobile device management: (1) use a messaging server's management capabilities (sometimes from the same vendor that makes a particular brand of phone); (2) use a product from a third party, which is designed to manage one or more brands of phone. GSA has implemented the latter approach with the use of the Google MDM (as part of Google Apps for Government) and the cloud based, MaaS360 MDM by Fiberlink, Inc.

Below is a summary of how GSA is addressing the strategic goals as listed in NIST SP 800-124:

Organizations should have a mobile device security policy – The details are documented in this guide.

Organizations should develop system threat models for mobile devices and the resources that are accessed through the mobile devices – GSA uses MaaS360 to satisfy this requirement. MaaS360 has the ability to provide detailed software listings for all devices so that Administrators and Management are aware of applications in use. Additionally, any application found to provide an unacceptable risk to Enterprise data or assets can be restricted based on that threat, for both Android and iOS smartphones and tablets.

Organizations deploying mobile devices should consider the merits of each provided security service, determine which services are needed for their environment, and then design and acquire one or more solutions that collectively provide the necessary services

– GSA has determined that all devices (iOS and Android) must have MaaS360 AND Lookout mobile security to satisfy this requirement. As such, all devices are monitored to ensure once installed, they remain active and updated to provide an adequate level of security for all mobile smartphones and tablets.

Organizations should implement and test a prototype of any mobile device solution before putting the solution into production – All mobile devices must be tested by the Mobile Device team and/or the Office of the Chief Information Officer (OCIO), Information Systems Security Manager (ISSM). Subsequently, they must be approved for use by the OCIO, and ISSM, with a published configuration guide, before being issued to GSA users or approved for use under the Bring Your Own Device (BYOD) guidelines outlined in Section 4.2 of this document.

Organizations should fully secure each organization-issued mobile device before allowing a user to access it – MaaS360 must be provisioned and activated on a device before being approved in the Google Administrative console (CPanel) to allow the syncing of GSA data by the Mobile Device Team. This applies to both Government and approved personally owned devices.

Organizations should regularly maintain mobile device security – The OCIO, ISSM is charged with the periodic monitoring of all mobile devices and shall implement a methodology of weekly reporting that shall be archived for review and adjustment of the overall security strategy for mobile devices in GSA.

1.1 Purpose

The purpose of this guide is to outline how GSA centrally manages and secures mobile devices, such as smart phones and tablets and the applications loaded on them. This publication also explains the security concerns inherent in mobile device use and provides direction on securing mobile devices throughout their life cycle.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal Employees, contractors and associates of GSA issued a mobile device or who have a personally owned device approved to be in GSA's Bring Your Own Device (BYOD) program.

1.3 Policy

Securing Mobile Devices is covered in Chapter 4, paragraph 2 of CIO 2100.1 as stated in the following paragraphs.

r. Mobile devices (smartphones/tablets). GSA users must secure mobile devices, like all enterprise devices, against a variety of threats. This includes handling PII as described in Chapter 4, Paragraph 4, subparagraph w of this chapter, securing the devices, and reporting lost or stolen devices. Included in the definition of 'Mobile devices' are smartphones and tablets. Excluded in the definition of mobile devices are laptops since the security controls for laptops

are quite different from smartphones. Also excluded in the definition are basic cell phones due to the limited security options available and their limited threat. GSA has outlined information on mobile devices at: https://sites.google.com/a/gsa.gov/mobileinfo/. The IT Security Procedural Guide: Securing Mobile Devices and Applications, CIO-IT Security-12-67 is designated as the GSA policy on mobile devices and applications and provides specific information, including:

(1) Government issued devices.

(a) GSA uses centralized mobile device management (MDM) to manage the configuration and security of mobile devices. GSA provisions and activates MDM on each mobile device before issuing to users.

(b) GSA organizations must define procedures to periodically monitor mobile device security to verify compliance with GSA requirements.

(c) GSA's MDM ensures appropriate security including: encryption, application controls, passwords usage, remote locking, remote wiping, operating system protection.

(d) Users must not connect to GSA resources without complying with the requirements which the Guide describes.

(2) Personally owned mobile devices.

(a) GSA has implemented a Bring Your Own Device (BYOD) policy that allows users to connect non-GSA procured devices to GSA resources.

(b) IT Security Procedural Guide: Securing Mobile Devices and Applications, CIO-IT Security-12-67 is designated as the GSA policy on mobile devices and applications, and details the steps necessary to use a personally owned mobile device, which include:

1. *GSA will install MDM on the device and enforce control security settings, including password usage, encryption, and inactivity timeout.*
2. *GSA will ensure that GSA can wipe the device clean if it is lost or stolen or after repeated unsuccessful attempts at logon.*
3. *GSA will not support personally owned mobile devices.*
4. *Users must agree to and sign a GSA Personal Device Usage Agreement and the GSA Rules of Behavior for Personally Owned Mobile Devices.*

1.4 References

Federal Standards and Guidance:

- Public Law 113-283, *"Federal Information Security Modernization Act of 2014"*
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- NIST SP 800-124 Revision 1, "*Guidelines for Managing the Security of Mobile Devices in the Enterprise*"

GSA Directives, Policies, and Procedures

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Rules of Behavior for Personally Owned Mobile Devices

2 Mobile Device Management (MDM) Architecture

GSA implements a defense in depth concept in MDM with the use of the Google MDM feature set as well as the MaaS360 MDM platform for security of mobile devices in the Enterprise.

The security services provided by Google MDM and Maas360 provide the ability to implement security of the following categories identified in NIST SP 800-124. The list contains complete capabilities of the MDM platforms, however not all items listed have been configured for use as GSA's deployment of mobile devices is still being tested and developed. GSA's current settings are found as embedded documents at the end of this section and are boldfaced at the end of each bullet.

- **General Policy:** General policy restrictions of particular interest for mobile device security include the following:
  - Restrict user and application access to hardware, such as the digital camera, GPS, Bluetooth interface, USB interface, and removable storage.
    GSA policy - Not restricted and available for customer use
  - Restrict user and application access to the built-in web browser, email client, application installation services, etc.
    GSA policy - Not restricted and available for customer use
  - Manage wireless network interfaces (Wi-Fi, Bluetooth, etc.)
    GSA policy - Not restricted and available for customer use
  - Automatically monitor, detect, and report when policy violations occur.
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel
- **Data Communication and Storage:**
  - Strongly encrypt data communications between the mobile device and the organization. This is most often in the form of a VPN, although it can be established through other uses of encryption.
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies
  - Strongly encrypt stored data on both built-in storage and removable media storage. Removable media can also be "bound" to particular devices such that encrypted information can only be decrypted when the removable media is attached to the device, thereby mitigating the risk of offline attacks on the media.
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies
  - Remotely wipe the device (to scrub its stored data) if it is suspected that the device has been lost, stolen, or otherwise fallen into untrusted hands and is at risk of having its data recovered by an untrusted party. A device often can also

be configured to wipe itself after a certain number of incorrect authentication attempts.
GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies

- **User and Device Authentication:**
  - Require 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).
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies
  - 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.
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies
  - Have the device automatically lock itself after it is idle for a period (e.g., 5 -15 minutes).
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies
  - Remotely lock the device, if it is suspected that the device has been left in an unlocked state in an unsecured location.
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies

- **Applications:**
  - Restrict which applications may be installed through blacklisting (or whitelisting).
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel
  - Install, update, and remove applications.
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies
  - Restrict the use of synchronization services (e.g., local device synchronization, remote synchronization services and websites).
    GSA policy - Not presently restricted and available for customer use, but continually monitored for implementation by user devices/applications
  - Digitally sign applications to ensure that only applications from trusted entities are installed on the device and that code has not been modified.
    GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies and this guide
  - Distribute the organization's applications from a dedicated mobile application store.
    GSA policy - Available for use through MaaS360 for iOS and private channel for Android

- Limit or prevent access to the enterprise based on the mobile device's operating system version (including whether the device has been jailbroken/rooted) or its mobile device management software client version (if applicable).
  GSA policy - Configured and managed by MaaS360 and/or Google CPanel as well as device configuration policies

The MDM Policy Settings Google folder contains the following settings:

- Google Cpanel Settings - administrative console
- MaaS360 Android Policy – for Android devices
- MaaS360 iOS Policy – for iOS devices

3 GSA Mobile Device Site

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 at the following URL:

https://sites.google.com/a/gsa.gov/mobileinfo/

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
- Hardening instructions for all approved devices, both government and personal
- Mobile Device/Application policies
- Rules of Behavior for use of approved personally owned devices
- Provisioning Certification
- Use of the "Application Specific Password"
- An outline of policy for procurement of government mobile devices

This site is maintained by the Mobile Device Management team under the supervision of the Director of Applied Solutions, OCIO, and the ISSM who is charged with overall management of GSA's mobile device security strategy.

4 GSA Mobile Device Process

The following sections provide information on mobile devices, their lifecycle, and their procurement, implementation, and maintenance.

4.1 Definitions and Concepts of Mobile Devices

- A small form factor device, commonly known as smartphones or tablets running either the iOS or Android OS
- Encryption for the device and device storage

- At least one wireless network interface for Internet access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with Internet connectivity
- An operating system that is not a full-fledged desktop or laptop operating system
- Applications available through approved methods (provided with the operating system – Apple ITunes and Google Play respectively). Installation of applications from unknown sources is not authorized. These unknown sources include third party application sources, such as the Amazon App store.
- Built-in features for synchronizing local data with a remote location (desktop or laptop computer, organization servers, telecommunications provider servers, other third party servers, etc.), unless specifically approved by GSA, is not authorized.
- Direct loading of data via direct connection between authorized mobile devices with GSA issued GFE is authorized.
- Network services:
    - One or more wireless personal area network interfaces, such as Bluetooth or near-field communications,
    - One or more wireless network interfaces for voice communications, such as cellular,
    - Global Positioning System (GPS), which enables location services.
    - Dual network connections is not authorized
- One or more digital cameras
- Microphone
- Encrypted Storage/movement of data to/from GFE:
    - Support for removable media
    - Support for using the device itself as removable storage for another computing device.

4.2 GSA's Bring Your Own Device (BYOD) Policy

GSA has implemented a BYOD policy that allows users to connect their non-GSA procured devices, which have been previously approved by IT security, to GSA resources in a native fashion. This presently does not include laptops, only smartphones/tablets. There should be no expectation of reimbursement to the user by the Federal Government when this policy is enacted at the request of a user for either the cost of the device or the wireless service running on it. GSA will not pay for the replacement or repair of any personally owned devices even if they are used for work purposes. The BYOD Program is strictly voluntary. Employees may choose to use their personal mobile device for work, but no one is required to do so. GSA will provide the Government Furnished Equipment (GFE) needed to meet the needs of each employee's work. Use of personally owned devices in addition to, or instead of, GFE is the employee's choice, under management discretion. The following guidelines outline the current BYOD Policy for GSA employees and contractors:

- The user (owner of the personal device) must agree to and sign the Rules of Behavior (ROB) for personally owned devices found in Section 2.1.

- In signing the ROB, users understand the device will be managed using MaaS360 and all security settings/policies of government devices will be enabled on their device. Users acknowledge there is no expectation of privacy under BYOD.
- The user understands that if the device is lost or stolen, it must be immediately reported to the IT Service Desk upon discovery of the loss or theft.
- The user understands that the device may be wiped, if deemed necessary by GSA IT Security officials, without prior notification to the user.
- The mobile device should be protected in the same manner as a valuable personal item and should not be left unattended in public places, automobiles, etc.
- The user will not install, transfer or access classified information with the device.
- The mobile device shall automatically lockout within 15 minutes of inactivity. The session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication.
- The device will automatically wipe after 10 unsuccessful attempts at logon.
- The device will maintain a minimum passcode length of 6 characters.
- Encryption must be enforced on the device at all times.
- The device must support a remote wipe capability and be configured to allow remote wiping in the event the device is lost or stolen.
- The device's OS must be maintained and kept up to date, with such updates occurring not later than 30 days after release.
- GSA will not be liable for any loss of personal data due to a remote wipe required under any circumstance.
- The device owner is responsible for any and all maintenance, repairs, warranties, accessories and the like for their personally owned device.
- The GSA OCIO is not responsible for supporting personally owned devices or training users on the devices. There are Chatter Groups and Discussion Forums available to GSA users for various operating systems and hardware devices that can be of help when technical assistance is needed.
- GSA funding for devices/services may be allowed for certain exceptions to allow for Reasonable Accommodation or other special circumstances. OCIO will review requests for exceptions on a case-by-case basis.

4.3 Mobile Device Development 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. The phases of the life cycle are as follows:

Phase 1: Initiation. This phase is considered complete with the publication of this guide and all supporting documentation.

Phase 2: Development. In this phase, the OCISO and the OCIO, ISSM shall coordinate activities to outline new guidelines, security requirements, and best practices as they evolve. They shall be incorporated into this guide, the SOPs of operational staff and the Mobile Device site referenced in Section 4.4 below.

Phase 3: Implementation. In this phase, equipment is configured in accordance with published hardening guides and is managed utilizing the procedures outlined in Section 2 above.

Phase 4: Operations and Maintenance. This phase is outlined in Section 4.5 below.

Phase 5: Disposal. All mobile devices shall be either remotely wiped or local reset to factory defaults (under settings) for both internal storage and any/all media cards prior to excess or reissue to meet the requirements of this phase.

4.4 Mobile Device Acquisition Procedures

Procedures to acquire a mobile device can be found at:

https://sites.google.com/a/gsa.gov/mobileinfo/procurement-of-mobile-devices

OCIO will manage and provide technical support for smart phones and tablet devices within the current infrastructure support environment. Service and/or Staff Offices (SSO) 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. At the present time, OCIO has determined that there is no requirement for centralized acquisition of smart phones or tablet devices on an enterprise basis beyond what is provided under the current enterprise contract for no cost Android or iOS devices. The below decision tree provides high-level acquisition guidance; SSOs should consult with assigned counsel for advice on any acquisition where Trade Agreements Act issues may arise.

All smartphones and tablets must be assessed for security prior to approval and use by GSA users. This includes both Government furnished equipment and those implemented under the BYOD guidelines addressed elsewhere in this guide. This assessment is to be recorded using the GSA Mobile Device Assessment Form, signed and maintained by the ISSM for the Enterprise Mobile Devices (EMD) system. This assessment, once completed, should remain on file for review as long as devices of this type are in use throughout the Enterprise.

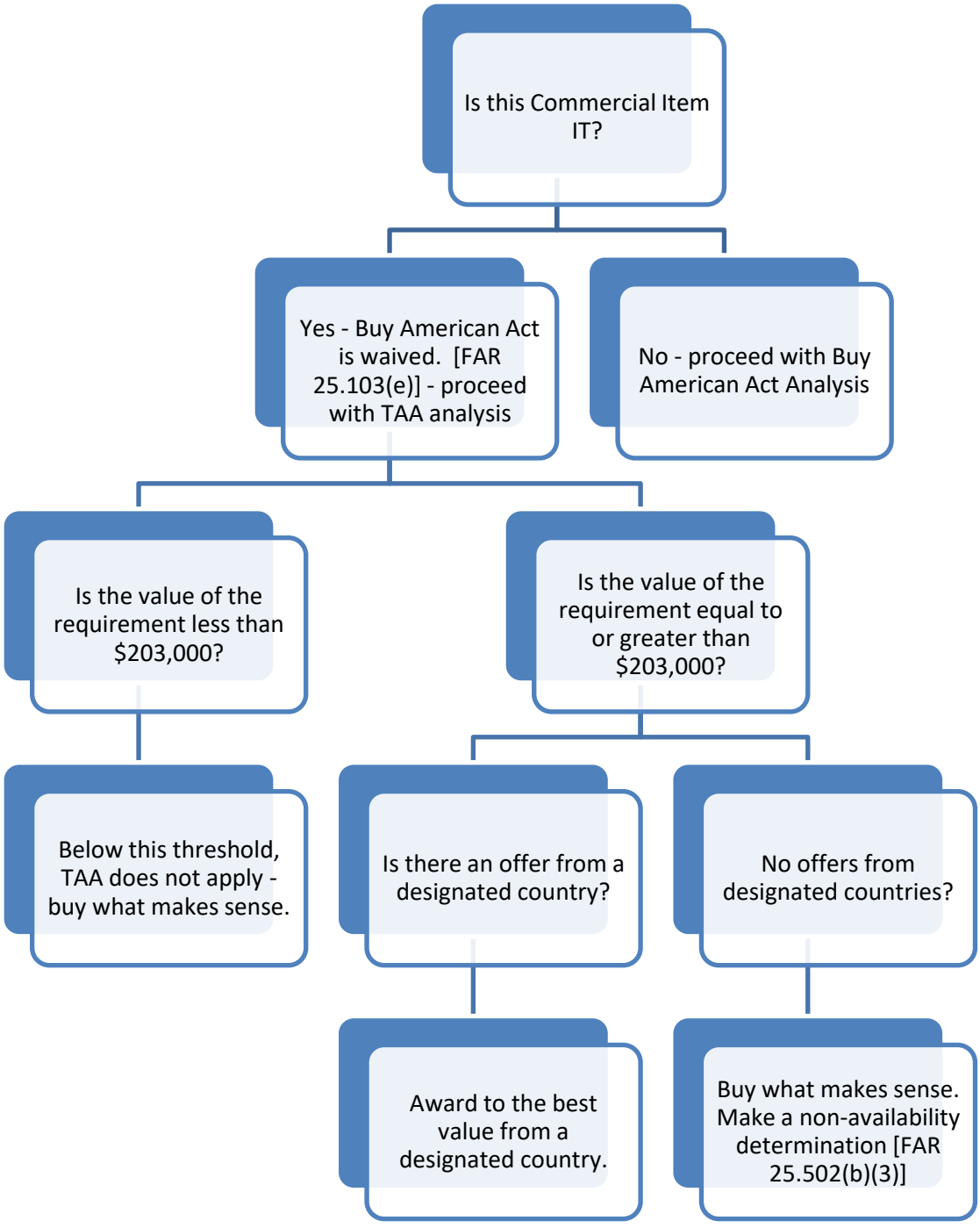

Figure 4-1: Mobile Acquisition Guidance

4.5 Mobile Device Operations and Maintenance

The OCIO staff is charged with the lifecycle maintenance of all mobile devices in GSA. This includes:

- Proper provisioning of all devices (both Government and personally owned) in accordance with applicable hardening guides and this publication
- Management of the MaaS360 and Google MDM platforms, configuration settings, administrator alerts, remote wiping of devices and application management
- Proper device wiping to sanitize media, including internal and external storage, on all devices prior to disposal or reuse.

5 Mobile Device Security Best Practice Resources

The security objectives of mobile devices are accomplished through a combination of security features built into the mobile devices and additional security controls applied to the mobile devices and other components of the enterprise IT infrastructure, as described throughout this guide and the Mobile Device site, as well as steps taken by end users. Additional resources available for administrators and users alike are listed below:

- United States Computer Emergency Readiness Team (US-CERT), "*Cyber Threats to Mobile Phones*"
- US-CERT TIP-10-105-01, "*Cyber Threats to Mobile Devices*"
- US-CERT ST04-017, *"Protecting Portable Devices: Physical Security"*
- US-CERT ST04-020, *"Protecting Portable Devices: Data Security"*
- US-CERT ST05-003, *"Securing Wireless Networks"*
- US-CERT ST05-017, *"Cybersecurity for Electronic Devices"*
- US-CERT ST06-007, *"Defending Cell Phones and PDAs Against Attack"*
- US-CERT Podcast Episode, *"Mobile Device Security: Threats, Risks, and Actions to Take"*

6 Providing Assurance of Security Controls

6.1 Google MDM Device Policy Settings

The documents at the links listed below provide a listing of the device configuration and policy settings for Mobile Devices that GSA/MaaS360 manages.

GSA_MDM_Android
GSA_MDM_iOS_DEP
Google Cpanel Settings

6.2 Mobile Device Inventory/Compliance Report

This process consists of maintaining an inventory of mobile devices connecting to Gmail, the goal being to report on compliance of these devices to GSA policy weekly and provide it to the

appropriate ISSM. The report is generated by comparing the data from MaaS360 to the configuration settings identified in the previous section. The report is maintained by the ISTE Assessment & Compliance Team.

A copy of the weekly report is to be forwarded to mobile-device-support@gsa.gov by the ISSM to certify it has been reviewed and any necessary actions have been coordinated with applicable Local Support and affected users.

7 User Compliance Requirements

A user may NOT connect a mobile device to GSA resources (Mail, Drive, VPN, etc.) or store ANY GSA data on any device (personally owned or government furnished) without complying with all aspects of this guide.

It is expected that all users, whether using government issued mobile devices or personally owned devices using the BYOD program, are to comply with all aspects of this guide. User compliance is mandatory and deviation from standards addressed here 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, whether issued a GSA owned device or a personally owned device under the BYOD program. 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 either the Google or MaaS360 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

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 apps for all devices, whether they are government owned or under the BYOD program. These settings/apps must be set by the user and not changed/removed at any time.

For Android devices:

- "Jailbreaking" or "rooting" of a device is not allowed
- All devices must have the Lookout Mobile Security app loaded and kept up to date
- All devices must have the MaaS360 app 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:

- "Jailbreaking" or "rooting" of a device is not allowed
- All devices must have the MaaS360 app loaded and kept up to date
- All devices must have the MaaS360 Security Profile (in mail) loaded and kept up to date
- 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.

8 Mobile Device Applications

A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited capabilities and isolated functionality. The simplest apps are developed to utilize the web browser of the mobile device to provide a feature set integration much like what is found on a user's PC. However, as mobile app development has grown, a more sophisticated approach involves developing applications specifically for the mobile environment, taking advantage of both its limitations and advantages. For example, apps that use location-based features are inherently built from the ground up with an eye to mobile devices given that you do not have the same concept of location on a PC. With this new paradigm in both mobile platforms and the applications loaded on them, GSA will concentrate security focus on the following goals:

That all apps loaded have a policy in place (this guide) to accurately describe when an assessment by GSA for acceptability is required and then a security assessment & authorization, when deemed as a requirement.

- That all apps are deployed from only trusted sources, following their security/assessment process – This presently is the Apple ITunes store for iOS and the Google Play store for Android. MaaS360 may also be used, once retrieved from these sources, for enterprise deployment
- That Terms of Service (ToS) discipline is adhered to, based on acceptability of an app – either as an individual user or for GSA as an Agency
- That apps deemed to be unacceptable are blacklisted, using MaaS360
- That a mobile app inventory for all devices be maintained using MaaS360
- That GSA developed apps are assessed, evaluated and approved by the Authorizing Official for the system they support before deployment.

8.1 Application Working Group (MAWG)

The Mobile Device Team along with the Enterprise ISSM (ISTE) and staff are charged with doing an periodic review of all mobile applications deployed, as well as taking input from sources such as Lookout, Inc., DHS, Law Enforcement and other publicly dispersed assessments and providing recommendations to the CISO on improving the mobile device/application environment in GSA.

Then, based on that periodic review, make a recommendation to the ISTE that further review is required for approval for any specific app.

8.2 Mobile Application Review and Approval

Mobile apps are generally categorized, shown in the figure below, in the following manner:

- GSA (or other Agency) Apps that have undergone an assessment and authorization process by their Authorizing Official as outlined in GSA IT Security 06-30, Managing Enterprise Risk and have been published in either the ITunes or Google Play store. ***(Approved)***
- Apps that have undergone a review, ToS validation, security assessment and final approval by the GSA CISO. (***Approved)***
- Apps that required a review, ToS validation & security assessment and were deemed unacceptable by the CISO based on any/all of the criteria. **(Unapproved)**
- Apps that were determined not to require further ToS validation or assessment. **(Acceptable). These apps are still subject to periodic review by the Mobile Device Team and the Enterprise ISSM and staff, with the potential to cause them to be re-categorized in to one of the above categories.**

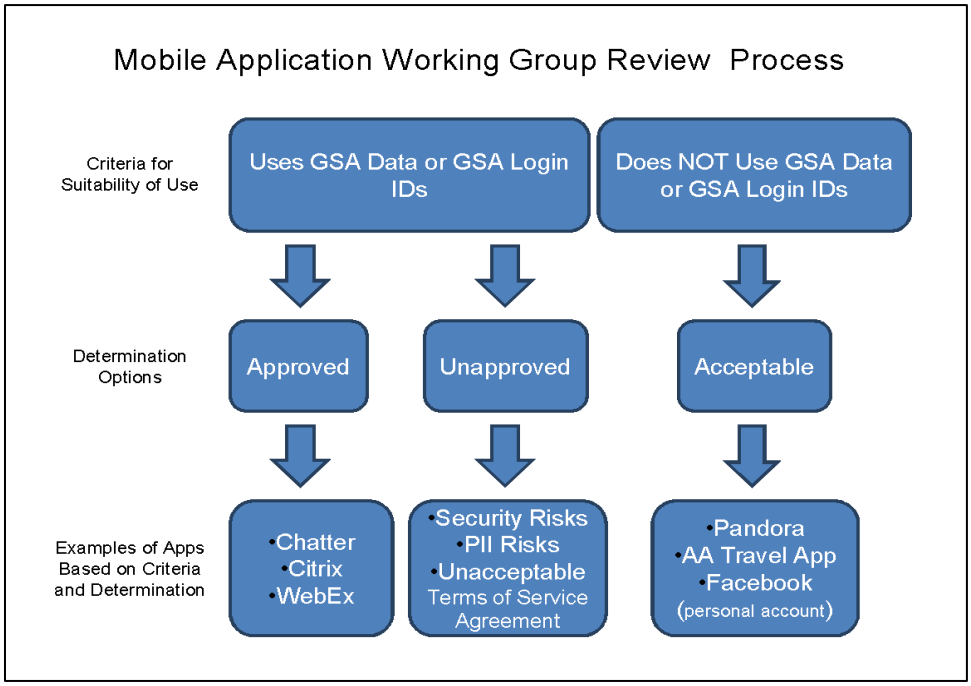

Figure 8-1: Mobile Application Working Group Review Process

The initial mobile app review performed by a user wishing to install an application, or any other party within GSA determines the above criteria based on whether the app itself might in some way compromise the integrity of GSA's network, user credentials or GSA data. In the initial review, a user performing the review physically loads the app onto a device to:

- Validate its function
- Verify accessibility to either the GSA infrastructure or data.
- Determine if GSA user credentials are required for the apps function.
- Determine if data is stored, is then placed in an unapproved location (such as an unauthorized cloud storage server farm).

If it is determined that the app in no other way violates GSA policy (i.e., pornography, gambling sites), or if used and is exposed to the general public, does not reflect poorly upon the individual as a Federal employee, the Government or GSA; that app is deemed to be acceptable for use by the individual following the ToS discipline outlined in Section 8.5. If the app is found to be using any/all of the above criteria, a formal assessment must be conducted, ToS formally negotiated or approved by General Counsel and an approval determination must be made by the CISO. If unapproved, the app is then blacklisted in MaaS360 by the Mobile Device team. Apps intended to be procured using Government funds must also undergo a full assessment, ToS validation and approval by the CISO. A process flow on the following page denotes this process.

The apps reviewed originate from two sources:

- A periodic review of the Mobile App Inventory taken from MaaS
- An app requested by a user to the Mobile Device team, or any IT security member of the GSA CISO's office

Once the app has been categorized and an assessment completed and/or approval has been received (if required), this status shall be noted to assist users in determining apps that are already allowed in the environment.

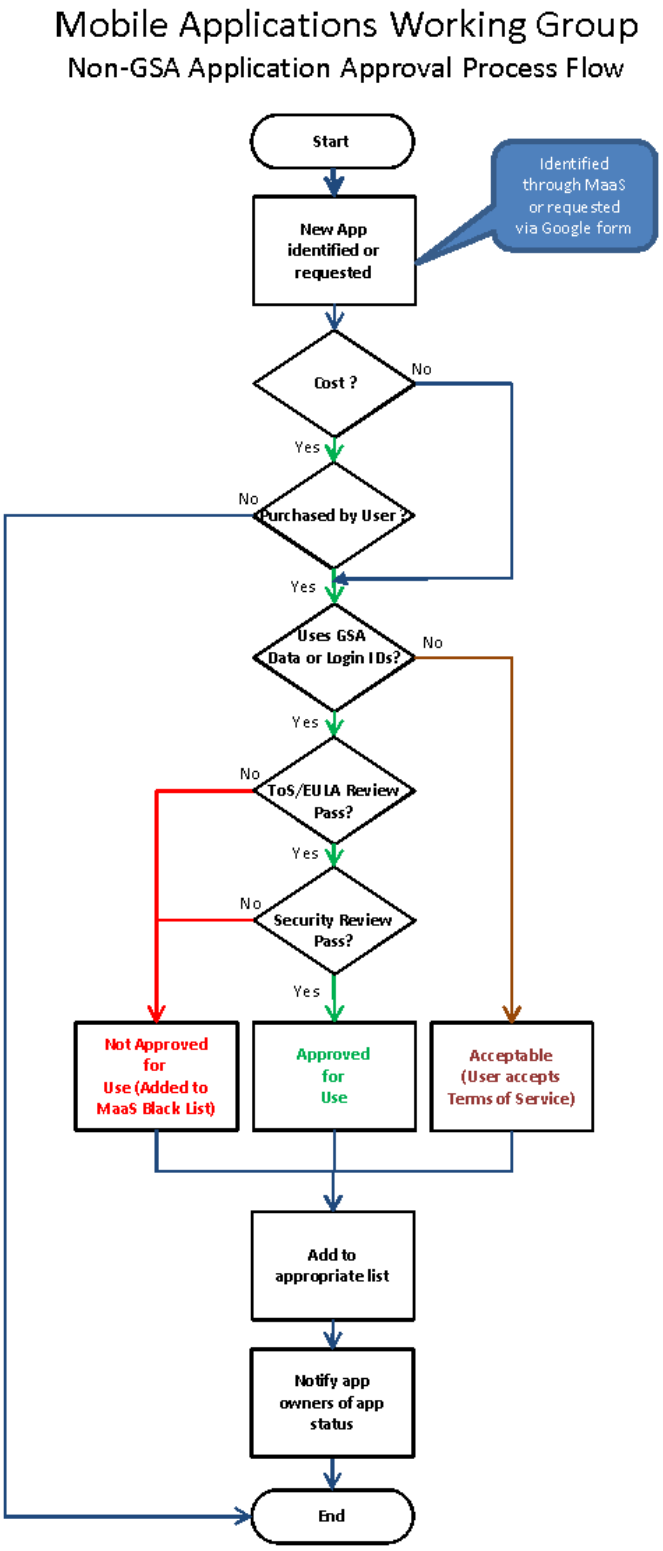

Figure 8-2: Non-GSA Application Approval Process Flow

8.3 Procurement of Mobile Apps

Apps may be purchased by users at their own expense, either for personal use or business related function. Refer to Section 8.2 above; if an app is not approved, that app will NOT be authorized for use on either GSA devices or personal devices allowed under the BYOD policies outlined in Section 4.2 of this guide. There should be no expectation of reimbursement by GSA to the user under any circumstance if personal funds are used to procure an app, whether that app is approved for use or not.

As mobile apps today are normally developed for both Android and iOS platforms, acquisition of any specific OS branded app shall not be, in itself, sufficient cause for brand name justification in the procurement of specific types of devices.

Government purchase of apps for iOS and Android devices must follow normal internal controls and policies. Volume Purchasing Programs should be followed and purchases have to be coordinated with GSA's Mobile Device Team. Details of Apple's volume purchasing program can be found at the following link.

Apple's Volume Purchase Program

GSA does not participate in Google's volume purchase program as it requires the use of Android for Work across all enterprise managed devices. It has been determined the effort required to implement Android for Work exceeds the need currently for a volume app purchase program implementation for GSA's Android devices.

8.4 Application Sources

Allowing mobile apps to be loaded from an unknown source presents one of the greatest risks to GSA's environment when using mobile devices. "Side loading" of apps is a process where a user installs an application from a source other than the Apple ITunes store or Google Play store. If a user jailbreaks a device, side loading can occur as well. Jailbreaking, or rooting, is a process where an OS of a mobile device grants a user or application root level access to the OS. While iOS devices that are not jailbroken/rooted protect against sideloading, the Android OS allows a user to turn such protection on/off (allow unknown sources) if not managed by MDM. As such, the following policies apply to all GSA devices (Government and BYOD) used in the environment to protect against side loading of apps:

- Devices shall not be jailbroken/rooted by users or apps loaded by users. GSA's MDM solution shall immediately notify an administrator of all such incidents immediately for remediation
- Unknown sources shall not be enabled by users or applications. GSA's MDM solution shall immediately notify an administrator of all such incidents for remediation

- GSA developed apps may be sideloaded for testing purposes only on test devices, but production deployment of GSA developed apps may only be done via the policies outlined below for Apple iOS and Google Android. The GSA MaaS store may be employed for enterprise deployments, but only after the app has undergone the review/approval processes outlined below.

    - Apple ITunes App Review Guidelines
    - Google Play Store App Review Guidelines

8.5 Terms of Service (ToS) and Privacy Discipline

Many terms found in commercial TOS or End User License Agreements (EULA) is not acceptable when the Government is the end user. OCIO requires that software and services within the GSA Enterprise have approved TOS or EULA.

Apps deemed to be acceptable: are loaded at the discretion of the user for either personal use or as a personal productivity tool to further enhance the work experience. As such, use of the app is not mandated by the agency and therefore acceptance of the ToS falls upon the user as an individual. This is true even if the app is loaded using a gsa.gov domain account or registered with a user's gsa.gov email address.

Apps that are approved after formal assessment: and include a formal review by GSA Counsel as part of the review/approval process, where the ToS was found to be acceptable to the government or a modified ToS was negotiated as part of the approval review, prior to final authorization. When loaded and activated, the user is accepting the ToS (often a technical function required of the user), not as an individual, but as an employee or contract employee assigned to perform work functions for GSA.

Privacy considerations must be addressed for commercial applications and applications developed by GSA for use by GSA personnel or for the general public.

As such, the following guidelines are to be adhered to:

Commercial applications – When reviewed for acceptability, consideration should be given to whether Personally Identifiable Information (PII) is collected. The app developer/sponsor should complete and submit a Privacy Threshold Assessment (PTA) to the GSA Privacy Office. This review will help ensure an adequate privacy notification is given to users prior to their installation and use of the app. Such notification should at a minimum include links to what data is being collected and for what purposes, as well as how it might be disclosed by those collecting it.

If the app collects, maintains or disseminates 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.

GSA developed applications – A GSA developed mobile app should undergo all the same reviews, procedures, and practices given to any developed application on any other platform. This should be documented in the PIA and System Security Plan for which the mobile app is a part of and a Privacy Notice must be included on the home screen of the mobile app itself.

If the app does NOT collect PII, at a minimum, the Privacy Notice should indicate that to the user. This can be done by taking the user to another screen on the app prior to launch, or by any means that allows a user to close the app prior to use before they are taken to an interactive screen.

If the mobile app DOES collection PII, the following minimum guidelines should be adhered to:

- The app must provide a Privacy Policy that is easily accessible to users through the commercial app store before installation as well as within the app, itself, after installation. This Privacy Policy should be app-specific and cannot merely reference the GSA website Privacy Policy (see below for an example/template).

- The Privacy Policy should briefly describe the app's information practices to include the collection, use, sharing, disclosure, and retention of PII or other sensitive information.

Privacy Notice

This mobile application does collect 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.

8.6 Inventory and Application Blacklisting

MaaS360 will be the authoritative source for mobile app inventory, by device and version history. This inventory will be used by the MAWG in their ongoing application review/assessment program outlined in Section 8.1 above for both iOS and Android platforms. It will also be used to review the overall health of the application security program by the OCISO and OCIO, ISSM.

Application blacklisting is a function of the MaaS360 platform and shall be managed by the Mobile Device Team under the direction of the OCISO and the OCIO, ISSM. If an app is blacklisted with current deployments already existing on devices, it is the responsibility of the Mobile Device Team to coordinate its removal with the user.

8.7 GSA App Development, Assessment, Authorization and Deployment

GSA developed apps are designed to take advantage of the concept of Anytime, Any Where, Any Device (A3) to allow GSA users and customers to access GSA data while mobile. As such, as GSA business lines develop apps for use on the iOS and Android environment, these apps must

undergo an assessment and authorization process before being deployed. With that in mind, the following guidelines are to be followed:

- A GSA developed app that supports a GSA Federal Information Security Modernization Act of 2014 (FISMA) system must be documented in the System Security Plan and authorized to operate as part of a current ATO letter from the respective AO before deployment. IT Security Procedural Guide CIO-IT 06-30, "Managing Enterprise Risk", is to be followed for this process. Any app that is not directly tied to an already existing system authorized to operate must have an assessment performed and subsequently approved for release by the CISO.
- Any mobile app development shall result in a minimum of the release of both an iOS and Android version of the app. This ensures coverage to all users within GSA and the maximum coverage for apps released to the public. Any additional application versions for alternate OS mobile platforms may be developed for such apps, but iOS and Android shall remain as the core base OS' for GSA developed mobile apps for all releases.
- All GSA developed apps must follow the respective application review and publication guidelines for the OS to which they were developed as outlined in Section 8.2 above as well as the release process documented at the end of this section.
- Other than for testing purposes on non-user provisioned mobile devices, side loading of apps in the environment is not authorized.
- The GSA MaaS360 Store is authorized for enterprise deployment of apps to GSA user devices once that app has been assessed, authorized and published according to the guidelines outlined in this section.
- Mobile code scanning throughout the development cycle is critical, but before release by the Mobile Device Team, a mobile app must be scanned by the ISE (SecEng) Team within the OCISO. This scan is a source code scan using the CheckMarx platform. As with all applications in GSA, no High/Critical findings are allowed from these scan results. Moderate findings should be documented in the respective POA&M for the system by which the app is authorized and accepted by the AO; Low and Informational findings should be taken into consideration by the developers for their next iteration of app development. A detailed process for mobile app release is documented at the end of this section.
- All mobile application development should take into consideration the OWASP Mobile Security Project in developing mobile apps either within GSA or for use by the general public.
    - OWASP Security Testing Guide
    - OWASP Mobile Security Project Home Page
    - OWASP Security Testing Guidelines for Mobile Apps
- GSA developed mobile apps must undergo an assessment review and approval process before being released for use. These apps fall into two categories that have slightly different processes for approval, with many common steps.
    - **Mobile apps that are developed as part of another system** with a current ATO and provide access to an application using a different form factor (smartphones/tablets). As stated above under Section 8.7, number 1, aside from

the common steps outlined below, such apps must be documented in the System Security Plan for the system they support.

- **Mobile apps designed for a specific purpose that are not part of a current ATO** and therefore, stand alone in their authorization to operate. As these apps do not have a parent system they support, the below listed process is the complete assessment process required for these apps.

- Common to both approval processes, all apps must
  - Be scanned prior to release by the ISE Division of the CISO using the Checkmarx Application scanner. No Critical/High findings may remain for approval to be received and any moderate/medium findings must be contained in a POA&M, either for the system the app is a part of, or a separate POA&M if a standalone mobile app.
  - Have a PTA/PIA completed and if applicable, tied to either an existing SORN or have a new SORN initiated and approved by the GSA Privacy Office and Office of the General Counsel.
  - A mobile application security assessment review must be completed and signed by the mobile app owner, mobile app assessor, mobile app ISSSM, a representative of the IST division of the OCSIO and a representative of the ISE division of the OCISO, to denote a proper assessment and review was conducted of the mobile app prior to release.
  - The full process for successfully completing steps 1-3 above are linked below Process to assess Mobile Applications in GSA