# Mobile Security Reference Architecture

May 23, 2013

**Product of the**
**Federal CIO Council**

**and**

**Department of Homeland Security**
**National Protection and Program Directorate**
**Office of Cybersecurity and Communications**
**Federal Network Resilience**

# Revision History

| Date | Version | Description | Approved By |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# Table of Contents

# Index of Figures

# Index of Tables

# Executive Summary

The Mobile Security Reference Architecture (MSRA) is a deliverable of the Digital Government Strategy (DGS). A key objective of the DGS is to procure and manage mobile devices, applications, and data in smart, secure, and affordable ways. The MSRA has been released by the Federal CIO Council and the Department of Homeland Security (DHS) to assist Federal Departments and Agencies (D/As) in the secure implementation of mobile solutions through their enterprise architectures. The MSRA document provides a reference architecture for mobile computing, including:

- Components of a mobile computing reference architecture;
- Categories for users of a mobile computing architecture;
- Sample implementations of a mobile computing architecture;
- Management and security functions of a mobile computing architecture;
- A discussion of the threats to mobile computing devices and infrastructures, and potential mitigations for those threats;
- Information assurance controls that apply to the mobile infrastructure components, and their relation to NIST Special Publication 800-53 rev4;
- A set of considerations for High Risk environments; and
- A discussion of the policy considerations necessary for the secure adoption of a mobile solution.

The MSRA is a flexible architecture designed to be adapted to fit the needs of any Department or Agency. Readers of the MSRA document should understand the role of each component in an architecture and the associated controls and management functions. This knowledge will allow a D/A IT architect to design a "best fit" solution for their enterprise and provide a solid set of security principles and controls to secure that solution.

One constant of the mobile computing world is the continual change and advancement of mobile technologies. In response to the evolving mobile technology landscape, the MSRA was designed to be a living document. The MSRA will be periodically updated to offer timely guidance on the implementation of new mobile technologies as they emerge.

# 1. Introduction

In 2011, Executive Order No. 13571 was issued to Federal Government agencies to improve the quality of services to the American people. As a result of this directive, the strategy document *"Digital Government: Building a 21st Century Platform to Better Serve the American People"* was created. As part of this strategy, the Department of Homeland Security (DHS), the Department of Defense (DoD), and the National Institute of Standards and Technology (NIST) were tasked with developing a reference architecture that would provide guidance to Federal agencies implementing mobile security. DHS, in collaboration with over 30 agencies, bureaus, and agency sub-components, developed a Mobile Security Reference Architecture (MSRA) to help Federal civilian agencies meet this directive and to help ensure privacy and security in the digital age.

Mobile computing devices ("mobile devices") require a rethinking of the security models that are traditionally employed to protect information accessed by off-site/remote workers. Appropriate authentication methods, traditional security products (e.g., anti-virus, firewalls), and connectivity options may be limited, nonexistent, or require modifications to accommodate mobile devices. The MSRA enumerates these issues and describes strategies to address them.

Prior to the adoption of mobile computing devices for processing Department and Agency (D/A)-sensitive information, D/As should perform a threat and risk assessment that is tailored to their specific mobile data threat environment and mobile services. Both policy development and the required levels of mobile device management should be considered as inputs to the threat and risk assessment so that D/As can implement appropriate security controls.

# 2. Architecture Scope

This Mobile Security Reference Architecture document focuses on securing the use of commodity mobile computing devices and infrastructures used to access Federal Government resources. The MSRA provides a review of the security risks associated with mobile computing devices and infrastructures, and example solutions for mitigating those risks. Although the MSRA primarily focuses on Government Furnished Equipment (GFE), a discussion of security concerns related to non-GFE devices is also provided.

This document primarily covers security concerns associated with mobile computing technologies and their related use cases. The use cases presented in this document cover mobile device data security, mobile device management (MDM), mobile application management (MAM), additional support infrastructure, and other specific technologies related to mobile computing devices. The MSRA presents the architectural components necessary to serve D/A user communities and to provide the data confidentiality, integrity, and availability that is critical to Government mission success.

The sample implementations presented in this document are designed to be used as a reference template for the adoption of mobile computing solutions within the Federal Government, though some tailoring by D/As will be required. Using these reference templates will help D/As save time and resources when planning the addition of a mobile computing infrastructure to support their missions and increase the security of the resulting solution. Security concerns related to the existing D/A infrastructures (e.g., database servers, web servers) are assumed to be well understood and are not discussed in this document.

Although it is outside the direct scope of this reference architecture, a discussion of policy concerns related to the implementation and use of mobile computing solutions is found in Appendix G.

The MSRA is intended to be a living document, meant to address the need for data security on mobile devices across the Federal Government. As technologies for mobile device management, identity verification, user authentication, data protection, and others continue to develop, the MSRA will be revised to include updated guidance and sample implementations.

## 2.1 Assumptions and Constraints

The following assumptions and constraints were used in the development of this reference architecture:

### 2.1.1 Assumptions

1. Mobile devices include smartphones and tablet computers. Laptops, including netbooks, are not covered by this reference architecture.
2. Mobile devices that access Government resources or process Government data are subject to Federal Information Processing Standards (FIPS), specifically FIPS 140-2, FIPS 199, FIPS 200, and FIPS 201.

3. Data categorization and marking guidelines are in place within the D/A, and information is being labeled/handled properly.
4. Trusted vendor and supply-source or procurement channels are established and used by the D/A.
5. Technology integration plans, such as needs assessments, specific use cases, pilot programs, roll-out, maintenance, and operations are the responsibility of the individual D/A, and should take the MSRA into consideration.

### 2.1.2 Constraints

1. The MSRA will not include capabilities unique to a single vendor.
2. The MSRA will not focus on specific operating systems or versions.
3. Some mobile operating systems cannot currently be managed by the components listed in the MSRA, and may be more appropriately managed by commercial enterprise host management solutions.
4. The MSRA is technology/Operating System (OS)-neutral, but examples and some features and vulnerabilities are technology/OS-specific.
5. Technology/OS features and capabilities change and are enhanced continuously. The MSRA is designed to be a living document that can incorporate these changes to security capabilities as they occur.
6. The MSRA will refer to mobile devices not provided by the D/A using the general term “non-GFE” rather than “bring your own device (BYOD)” since the devices may, in fact, be contractor provided and not the property of the individual user.
7. Security for mobile devices and supporting networks used to access National Security or Emergency Preparedness priority services (Government Emergency Telecommunications Service and Wireless Priority Service) is not fully addressed in this document.

# 3. Mobile Security Conceptual Architecture

The primary purpose of the MSRA is to provide an architecture pattern that D/As can use to ensure the confidentiality, integrity, and availability of data accessed through a mobile computing solution. To provide the maximum level of interoperability, the MSRA includes features from other Federal mobile security initiatives. Figure 1 shows the mobile security reference architecture.[1]

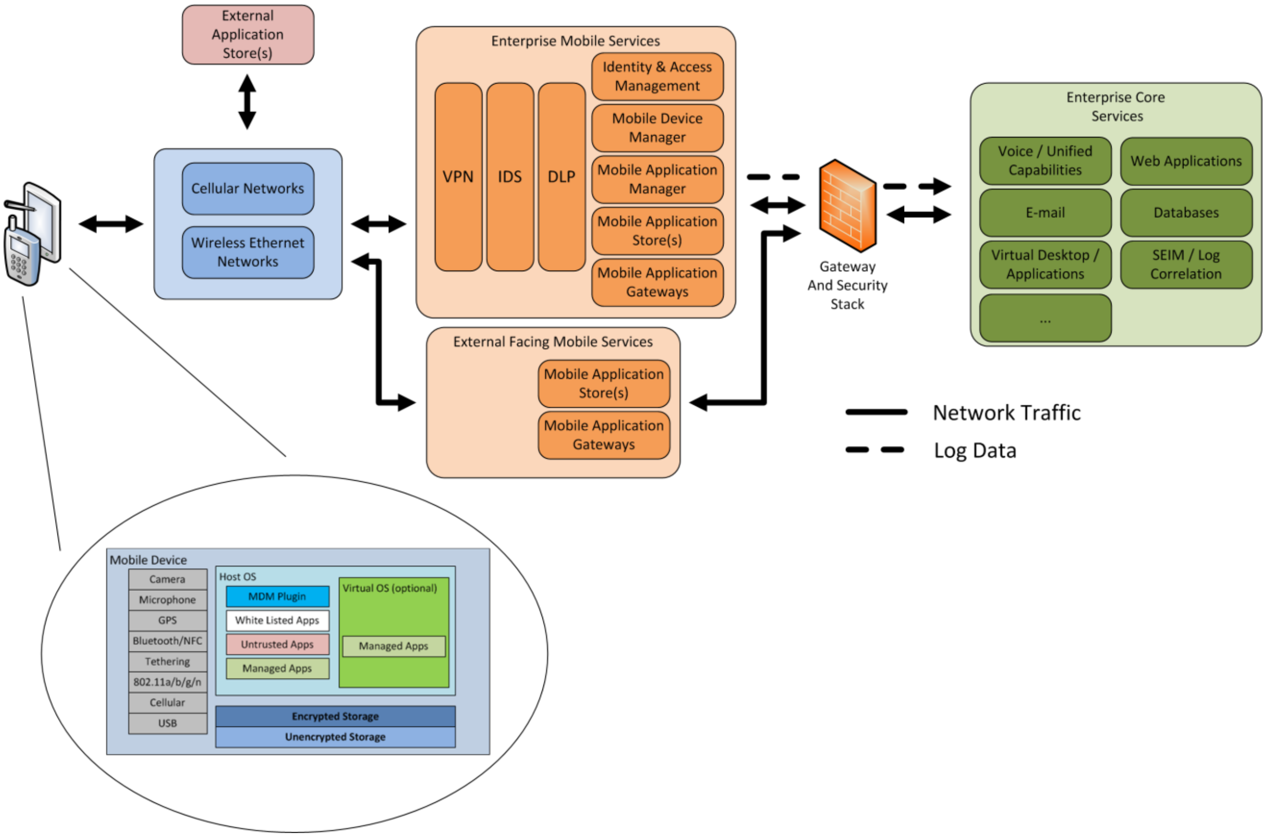
External Application Store(s)
Cellular Networks
Wireless Ethernet Networks
Enterprise Mobile Services
VPN
IDS
DLP
Identity & Access Management
Mobile Device Manager
Mobile Application Manager
Mobile Application Store(s)
Mobile Application Gateways
External Facing Mobile Services
Mobile Application Store(s)
Mobile Application Gateways
Gateway And Security Stack
Enterprise Core Services
Voice / Unified Capabilities
Web Applications
E-mail
Databases
Virtual Desktop / Applications
SEIM / Log Correlation
...
Network Traffic
Log Data
Mobile Device
Camera
Microphone
GPS
Bluetooth/NFC
Tethering
802.11a/b/g/n
Cellular
USB
Host OS
MDM Plugin
White Listed Apps
Untrusted Apps
Managed Apps
Virtual OS (optional)
Managed Apps
Encrypted Storage
Unencrypted Storage

*Figure 1: Mobile Security Reference Architecture*

This model[2] is also in line with other portions of the Digital Government Strategy, such as the Government Mobile and Wireless Security Baseline[3]. Of the areas shown in the mobile reference security architecture, the portions that are under the direct control of an organization are the mobile device infrastructure (shown in orange), the mobile device, and the applications that run on the mobile device. The enterprise mission services (shown in green) are also under D/A control, but are out of

[1] Components of the MSRA are also defined in the NSA Mobility Capability Package v2.0: http://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_2_0.pdf.

[2] This reference architecture is intended to illustrate the most common, single instance use of each component. It is up to the D/A to tailor the architecture to fit their needs.

[3] "Government Mobile and Wireless Security Baseline", Federal CIO Council (http://cio.gov).

scope for this reference architecture. Communications security is considered a function of the mobile device or its applications, and will be discussed in section 4.5 and Appendix B. The mobile device reference model, shown in the focus circle, is discussed later in Section 3.2.

This architecture serves as a baseline to guide agencies to securely and efficiently implement mobile security infrastructures. Section 3.1 describes the major components of the MSRA. Section 3.2 defines a set of use cases for mobile devices, and Section 3.3 presents sample implementations of the MSRA. Agencies should use a risk-based approach to modify this architecture for their specific needs.

## 3.1 Mobile Infrastructure: Architecture Components

The purpose of an enterprise mobile device infrastructure is to provide mobile computing devices secure and assured access to enterprise resources, and to protect the services to and data access by mobile clients. Mobile device infrastructures typically support three user categories: D/A users, partner users, and external users.

*D/A users* are employees of an organization that access organizational data and services from a mobile device. The determination of this need is typically predicated on the mission(s) supported by the employee, the sensitivity of the data the employee must access, and the need to access that data from non-organizational locations. D/A users are typically provided a set of mobile credentials that they use to access the organization’s internal systems.

*Partner users* are employees of organizations that partner with the D/A to fulfill a specific mission, including contractors that support a specific D/A. Partner users may require access to D/A data, applications, and infrastructure to complete their assigned tasks, but are not afforded the same level of access and privilege as authorized employees. Partner users are typically provided a set of mobile credentials that are used to access the organization’s internal systems.

*External users* are individuals not necessarily affiliated with the organization who have the need to access the organization’s public data through organizationally provided and maintained interfaces. These interfaces can be web applications, mobile device applications, or other implementation-specific mechanisms. External users are not usually required to have credentials to identify themselves to an organization. In some cases, organizational data interfaces can have a set of locally usable credentials that are valid only for the resource being accessed. Users in each category can come from a wide variety of sources, including the groups[4] defined in the “Government Mobile and Wireless Security Baseline” document. The groups defined in that paper are shown in Figure 2. Although the Mobile Security Baseline uses the term Corporate Owned, Personally Enabled (COPE), the MSRA groups that functionality with the Government Furnished, Dual Persona use case.

[4] User groups correspond roughly to the users of the use cases defined in the Government Mobile and Wireless Security Baseline.

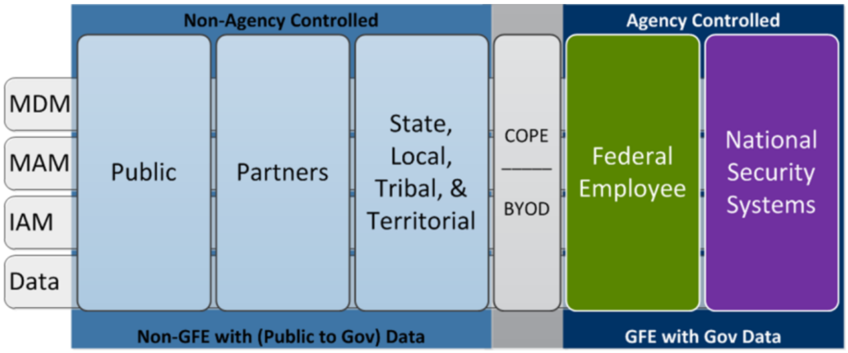

*Figure 2: Government Mobile and Wireless Security Baseline Defined User Groups*

To include these groups in their mobile computing solution, a D/A would have to determine how to characterize the members of each group as a user (e.g., D/A, partner, external) of their solution. Each type of user brings with it a widely varying set of mobile device hardware, only some of which can be effectively managed through Government mobile device management solutions.

Possible components of a mobile device infrastructure are described in the following sections. Table 1 identifies the components and the class of mobile user that is served by each. Due to the widely varied nature of mobile solutions, it is not possible to identify all potential components of a mobile solution; this reference architecture focuses on the most commonly used components.

| Component | D/A User | Partner User | External User |
|---|---|---|---|
| Virtual Private Network | ✓ | ✓ | |
| Mobile Device Management | ✓ | ✓ | |
| Mobile Application Management | ✓ | ✓ | |
| Identity and Access Management | ✓ | ✓ | |
| Mobile Application Store | ✓ | ✓ | ✓ |
| Mobile Application Gateway | ✓ | ✓ | ✓ |
| Data Loss Prevention | ✓ | ✓ | ✓ |
| Intrusion Detection System | ✓ | ✓ | ✓ |
| Gateway and Security Stack | ✓ | ✓ | ✓ |

*Table 1: List of Components by User Class*

Each of these mobile device infrastructure components is described below, with a reference to the security function(s) it provides. Selected security functions that apply to the management of a mobile computing solution's user base, listed in Table 2, are explained in Section 4.

| Mobile Security Function | Section |
|---|---|
| Authorization | 4.2.2 |
| Device Management | 4.4 |
| Diagnostic Data Management | 4.3.2 |
| Logging | 4.6.4 |
| Personnel and Facilities Management | 4.1 |
| Monitoring and Auditing | 4.6 |
| Network Access Control | 4.2.3 |
| Software Validation and Patch Management | 4.4.3 |

*Table 2: Mobile Security Functions Associated with User Management*

### 3.1.1 Virtual Private Networks (VPNs)

For mobile security, VPN technologies provide a robust method for creating secure connections between mobile devices and a D/A while using public unmanaged networks. VPN technologies are typically used only by authorized and partner users, but technologies exist that allow the ad-hoc establishment of VPN connections for external users. Not all paths need to traverse public networks. For example, a D/A can have a business relationship with a network service provider (NSP) that routes all mobile device data traffic from its internal networks directly to the D/A mobile device VPN concentrator without traversing publicly accessible networks. Table 3 lists the mobile security functions associated with VPNs.

| Mobile Security Function | Section |
|---|---|
| Personnel and Facilities Management | 4.1 |
| Secure Communications | 4.5 |

*Table 3: Mobile Security Functions Associated with VPNs*

### 3.1.2 Mobile Device Management (MDM)

Mobile Device Management is any process or tool intended to manage applications, data, and configuration settings on mobile devices. The intent of MDM is to centralize and optimize the functionality and security management of a mobile communications.[5] MDM is the primary mechanism for technical enforcement of D/A policies and procedures. Critical features include the scope of supported devices, platforms, and applications; the breadth of service providers it can function through; the targeting of single, group, and all mobile devices enrolled; the ability to support next-generation technologies quickly; the ease of enrollment and disenrollment of mobile devices; the security of the mechanisms used for device authentication, command and control; troubleshooting and diagnostic tool robustness; logging and reporting capabilities; completeness of the mobile device security parameters it is able to manage; and other features identified throughout this document. Not all MDM features will be applicable to all devices, as some features rely on specific hardware implementations that may vary

[5] For the definition of mobile device management, see http://searchmobilecomputing.techtarget.com/definition/mobile-device-management.

across devices, even those in the same family of devices. Table 4 shows the mobile security functions associated with MDM.

| Mobile Security Function | Section |
|---|---|
| Authorization | 4.2.2 |
| Configuration | 4.4.2 |
| Data Security | 4.3 |
| Device Management | 4.4 |
| Identity Access Management | 4.2 |
| Personnel and Facilities Management | 4.1 |
| Monitoring and Auditing | 4.6 |
| Secure Communications | 4.5 |

*Table 4: Mobile Security Functions for MDM*

### 3.1.3 Mobile Application Management (MAM)

Mobile Application Management provides a subset of the functionality provided by Mobile Device Management. MAM provides in-depth distribution, configuration, data control, and life-cycle management for specific applications installed on a mobile device. Like MDM, critical features of the MAM include the set of devices, platforms, and applications supported as well as the security of the mechanisms used for device authentication and command and control. MAM may also include diagnostic features, such as remote log-ins, reporting, and troubleshooting. Some MAM implementations are intended to support a small, specialized set of software, such as virtualized application containers (i.e., “sandboxes”), rather than being applicable to all applications on a device. Specialized MAM implementations may not integrate with more general MDM implementations, and thus are considered a separate component of a mobile solution. Table 5 shows the mobile security functions associated with MAM.

| Mobile Security Function | Section |
|---|---|
| Authorization | 4.2.2 |
| Configuration | 4.4.2 |
| Personnel and Facilities Management | 4.1 |
| Monitoring and Auditing | 4.6 |

*Table 5: Mobile Security Functions Associated with MAM*

### 3.1.4 Identity and Access Management (IAM)

Not all users of a mobile solution need access to the same data, have the same mobile device requirements, or use the same applications. Identity and Access Management systems are used to integrate services such as authentication and authorization across the mobile solution to form a cohesive security profile for each user. An IAM system enables the consistent application of a security policy across all mobile services and allows the integration of enterprise authentication and authorization systems with the mobile solution. For example, the use of an IAM system in conjunction with an MDM system allows each user of a mobile solution to have multiple devices (e.g., tablet and smartphone) configured with the same level of access and same security profile. IAM systems can also be used to enable synchronization of data across multiple devices and users. *Table 6* shows the mobile security functions associated with IAM.

| Mobile Security Function | Section |
|---|---|
| Identity and Access Management | 4.2 |
| Personnel and Facilities Management | 4.1 |
| Secure Communications | 4.5 |

*Table 6: Mobile Security Functions Associated With IAM*

### 3.1.5 Mobile Application Store (MAS)

A Mobile Application Store is a repository of mobile applications. Public application stores (i.e., External Application Stores) offer mobile applications for sale (or for free) to the public. Organizations can obtain software licenses to operate their own application store, available only to that organization's personnel. These "stores" provide a selection of approved applications that can be downloaded and installed on approved devices by the users of the device. Some MAS implementations can support multiple mobile platforms, but many are restricted to a single platform, requiring a D/A to operate multiple MAS's depending on the number and types of devices in use by the organization. The MSRA defines three types of MAS implementations, as shown in Figure 1. The External Application Store represents an application store that is run by an independent entity, over which the D/A has no control. The organization external application store represents a MAS run by the organization that is intended to offer mobile applications to the general public. The internal organizational application store represents a MAS designed to be used solely by the D/A's authorized users. An organization may need to run multiple MAS instantiations to support multiple user groups that function in different security domains (i.e., external user versus authorized users). Table 7 shows the mobile security functions associated with MAS.

| Mobile Security Function | Section |
|---|---|
| Personnel and Facilities Management | 4.1 |
| Traffic Inspection | 4.6.1 |

*Table 7: Mobile Security Functions Associated With MAS*

### 3.1.6 Mobile Application Gateway (MAG)

A Mobile Application Gateway is a piece of software that provides application-specific network security for mobile application infrastructures. The purpose of a MAG is to act as a network proxy, accepting connections on behalf of the application's network infrastructure, filtering the traffic, and relaying the traffic to mobile application servers. This proxy relationship allows the MAG to apply application layer filters to network traffic, providing focused security designed to protect the mobile application service. MAGs are often used in place of traditional network protections, such as intrusion detection systems, when application traffic is encrypted or opaque in structure. A MAG is traditionally conceptually separated from the Gateway and Security Stack because it functions at the application layer, rather than at the session and lower layers, as defined by the Open System Interconnection (OSI) Network Model. As shown in Figure 1, an organization may need to run multiple MAG instantiations to serve multiple user groups that function in different security domains (i.e., external user versus authorized users). *Table 8* shows the mobile security functions associated with MAGs.

| Mobile Security Function | Section |
|---|---|
| Personnel and Facilities Management | 4.1 |
| Monitoring and Auditing | 4.6 |

*Table 8: Mobile Security Functions Associated With MAG*

### 3.1.7 Data Loss Prevention (DLP)

Mobile infrastructure data loss prevention focuses on preventing restricted information from being transmitted to mobile devices, or from mobile devices to unauthorized locations outside the organization. A DLP solution monitors all traffic flowing to mobile devices from the organizational infrastructure, validating the traffic against a set of pre-defined words, phrases, images, and patterns that are considered too sensitive to leave the enterprise boundary. DLP solutions may also be configured to monitor traffic sent from mobile devices to entities outside the enterprise boundary. Traffic that contains sensitive information is either blocked or logged for future investigation. Table 9 shows the mobile security functions associated with DLP.

| Mobile Security Function | Section |
|---|---|
| Data Security | 4.3 |
| Monitoring and Auditing | 4.6 |

*Table 9: Mobile Security Functions Associated With DLP*

### 3.1.8 Intrusion Detection System (IDS)

An IDS is a network appliance that uses a set of heuristics to match known attack signatures against incoming network traffic and raises alerts when suspicious traffic is seen. Some IDS systems identify regular network traffic patterns using network flow data and can raise alerts when deviations from those patterns occur. An IDS is used in the reference architecture to detect potentially malicious activity from connected mobile devices. Table 10 shows the mobile security functions associated with IDS.

| Mobile Security Function | Section |
|---|---|
| Diagnostic Data Management | 4.3.2 |
| Monitoring and Auditing | 4.6 |

*Table 10: Mobile Security Functions Associated With IDS*

### 3.1.9 Gateway and Security Stack (GSS)

Mobile devices, like almost all computing devices, have the capacity to be used to attack other networked devices. The unique dual-connected nature (cellular and wireless Ethernet) of mobile devices makes them ideal platforms for circumventing traditional network security boundary protections. To prevent damage to the enterprise from a compromised mobile device, access to the enterprise must be restricted through one or more known network routes (i.e., Gateways) and inspected by standard network defenses such as stateful packet inspection, intrusion detection, and application and protocol filters. These standard defenses are collectively known as a “filter stack” because they serve to filter unwanted network traffic and are usually configured in a “stack” with traffic traversing each filter in sequence. The GSS typically functions at the session and below layers of the OSI network model. Table 11 shows the mobile security functions associated with the Gateway and Security Stack.

| Mobile Security Function | Section |
|---|---|
| Content Filtering | 4.6.3 |
| Packet Filtering | 4.6.2 |
| Traffic Inspection | 4.6.1 |

*Table 11: Mobile Security Functions Associated With GSS*

## 3.2 Mobile Devices and Applications

Hardware, operating systems, and application models can vary widely on commodity mobile devices. However, it is possible to construct a conceptual model that uses the commonalities between the platforms to describe a generic mobile device. This model is shown in Figure 3.

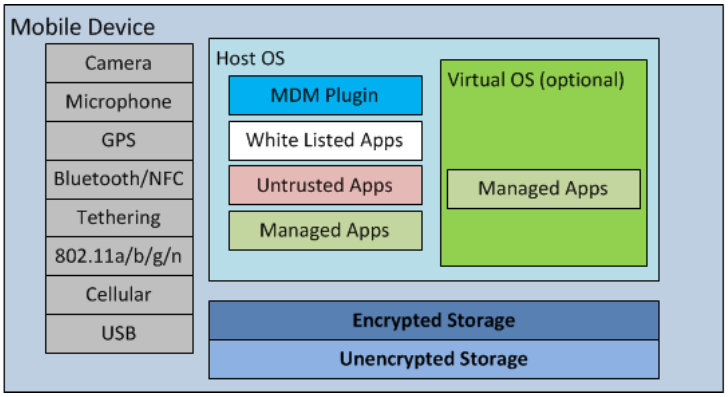

*Figure 3: Generic Mobile Device Model*

In general, a mobile device operating system runs each application in isolation using operating-system-specific mechanisms to regulate communication between applications. The controls available to regulate communication between applications vary widely across mobile operating systems, so it becomes important for the organization to understand the risks associated with inter-process communication.

Applications are granted access to device hardware components by the mobile operating system. Not all applications require access to all hardware components, and a risk-based approach should be taken to configure application access to hardware components. Similarly, encrypted storage access should be managed on an application-by-application basis to minimize the risk of data spillage. All data storage, encrypted or unencrypted, must conform to FIPS requirements, specifically those designated in FIPS 199, FIPS 200, and FIPS 140-2.

### 3.2.1 Mobile Device Use Cases

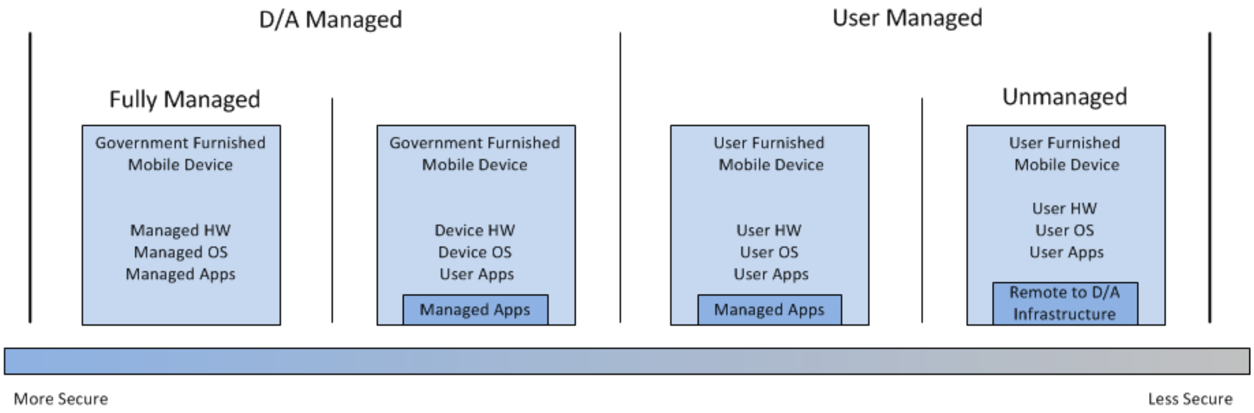

*Figure 4: Use Cases for Managing Mobile Devices*

Four basic use cases for managing mobile devices can be derived from the model shown in Figure 4. These use cases vary from a fully managed use case to a completely unmanaged use case. Although it is possible to derive a larger number of use cases, the four presented in Figure 4 represent the most likely cases for Federal systems. One mobile solution can support multiple device use cases, depending on the users the solution is intended to serve.

Some mobile device use cases assume the use of “Dual Persona” or device virtualization technologies. These technologies allow the device manager to create an isolated environment on the mobile device that has little, if any interaction with the device’s other functions. One type of isolated environment typically consists of a virtualized mobile operating system, storage, and application set. Because the virtual operating system functions identically to its non-virtualized counterpart, it may be configured and managed in the same way.

The host mobile operating system is required to allocate hardware devices to the virtualized operating system as necessary and may prevent the switching of devices between the virtualized and host environment to prevent data leakage or corruption of the isolated environment. The provisioning of a mobile virtualized environment is a very sensitive process and should not be subject to user control at any time in order to prevent potential misconfigurations that would compromise security.

Some Dual-Persona technologies do not function as an entire virtual operating system, but as an isolated “container” within the mobile environment. These containers are generated by a client application that runs on the mobile device and partitions space and resources to provide the necessary data separation. They virtualize the individual applications to be run, protecting them from outside influence through the use of an application level hypervisor. An application level hypervisor is an application designed to “wrap around” a specific mobile application. This “wrapper” intercepts system calls, library calls, and other OS interactions from the wrapped application, and adjudicates the calls based on a defined security policy. An application level hypervisor is typically very specialized, and implements only a fraction of the capabilities of an operating system level hypervisor. Switching between “personas” is then accomplished by launching the client software that manages the secure container.

### *Government Furnished, D/A Fully Managed*

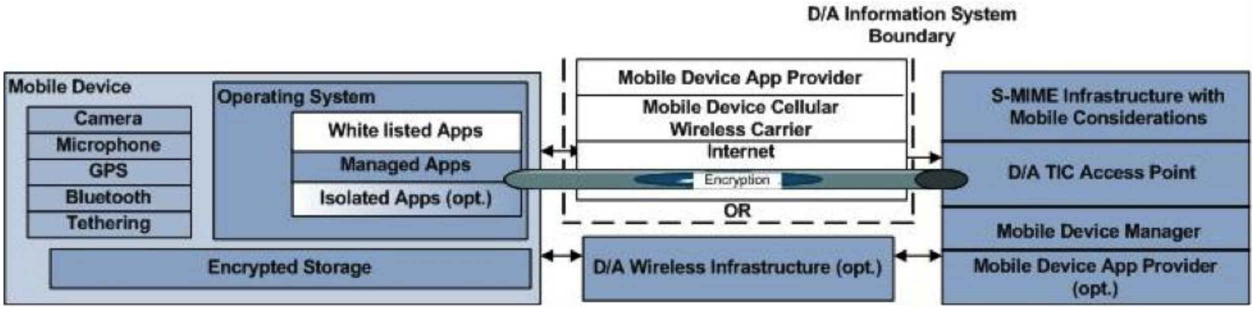
D/A Information System Boundary
Mobile Device
Camera
Microphone
GPS
Bluetooth
Tethering
Operating System
White listed Apps
Managed Apps
Isolated Apps (opt.)
Encrypted Storage
Mobile Device App Provider
Mobile Device Cellular Wireless Carrier
Internet
Encryption
OR
D/A Wireless Infrastructure (opt.)
S-MIME Infrastructure with Mobile Considerations
D/A TIC Access Point
Mobile Device Manager
Mobile Device App Provider (opt.)

*Figure 5: Fully Managed GFE Mobile Device Use Case*

Fully managed GFE Mobile devices, shown in Figure 5, offer D/As the greatest control over the user experience. In this implementation, the D/A controls the mobile service provider, mobile device hardware selection, operating system, applications (including version control), additional features of the mobile device that are enabled (e.g., camera, GPS, Bluetooth), storage controls, device disposal, and authentication techniques.

In this scenario, the mobile device can be treated as an extension of the internal network and be granted access to more sensitive information than in other mobile device architectures. Protection techniques that are used for remote teleworkers can be used on mobile devices to ensure proper data protections are preserved. This implementation provides the most business-feature-rich environment of the candidate architectures. However, the tradeoff is that this architecture is the least friendly for personal use. Personal use of the mobile device can be limited to a personal sandbox, provided that the users understand and agree that their data may be lost if device wiping is required[6]. Alternatively, a sandbox or application virtualization can be employed for hosting D/A information, which may be more sensitive than can be adequately protected by the device’s native security functions.

Some computing systems can be tethered to a mobile device in order to take advantage of the mobile device’s network connectivity. Although tethering may be allowed by D/A policies, there are risks that must be addressed. A tethered mobile device may be used as a way to bridge multiple networks, if the connected computing system has another network connection besides the tethered mobile device. In addition, a computing system tethered to a mobile device may be able to act as a part of the D/A network, despite the computing system not having authorization to do so. It is recommended that tethering be disabled while a mobile device’s VPN is in use.

[6] These issues should be addressed in user agreements and general counsel review, as described further in Chapter 4 of this document.

Control over device ownership allows the D/A to confiscate the device upon employee termination or reassignment, fully sanitize the stored information prior to disposal, conduct covert forensics and investigations, determine the lifespan of the device in use, and clear the device's memory contents in case of classified information spillage, without concern for the loss of the user's personal information. In addition, the D/A can enact appropriate use policies and prohibit the device from being used for personal business. Controls should be implemented to prevent a mobile device's multiple network access methods (e.g., cellular, wireless Ethernet) from being used to bridge an external network to an internal D/A network, or to bridge two internal D/A networks. In both cases, the bridge could be used to circumvent existing network safeguards, and to enable either attacks or network based information exfiltration. Additional guidance and information can be found in the National Security Agency's (NSA) Mobility Capability Package.

The principle drawbacks of this architecture are cost, complexity, and a lack of features for users' personal activities.

### Government Furnished, D/A Partially Managed, Dual Persona

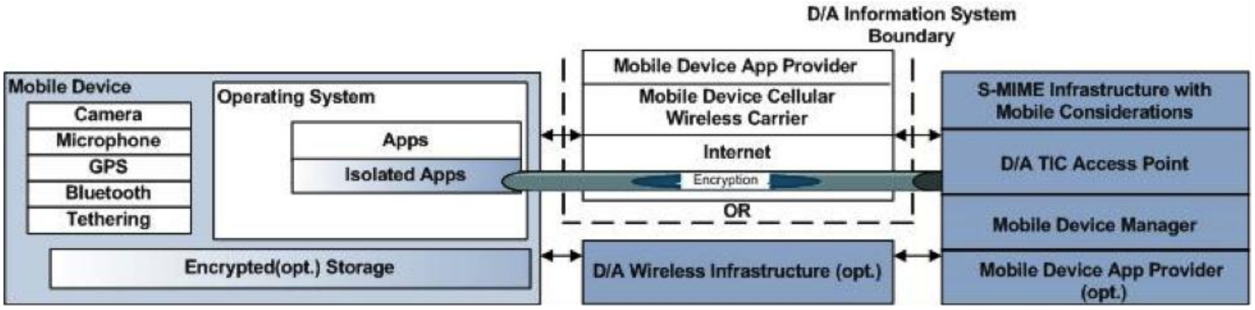
D/A Information System Boundary
Mobile Device
Camera
Microphone
GPS
Bluetooth
Tethering
Operating System
Apps
Isolated Apps
Encrypted(opt.) Storage
Mobile Device App Provider
Mobile Device Cellular Wireless Carrier
Internet
Encryption
OR
D/A Wireless Infrastructure (opt.)
S-MIME Infrastructure with Mobile Considerations
D/A TIC Access Point
Mobile Device Manager
Mobile Device App Provider (opt.)

*Figure 6: Government Furnished, D/A Partially Managed Use Case*

As depicted in Figure 6, this use case is predicated on the use of securely contained applications on GFE mobile devices. In the case of some mobile platform vendors, a vendor-provided device management system might not be available to manage the device at the OS level. For this reason and others, this use case represents a balanced approach to device management and control. By using application and storage virtualization on the mobile device, data with unique protection or authentication requirements can be locally stored and processed since the additional protections and authentication can be limited to the isolated data. Controls should be implemented to prevent a mobile device's multiple network access methods (e.g., cellular, wireless Ethernet) from being used to bridge an external network to an internal D/A network, or to bridge two internal D/A networks. In both cases, the bridge could be used to circumvent existing network safeguards, and enable either attacks or network based information exfiltration.

As with the fully managed mobile device implementation, this technique preserves D/A ownership of the mobile device, allowing the D/A to confiscate the device upon employee termination or reassignment, fully sanitize the stored information prior to disposal, determine the lifespan of the device in use, and clear the device's memory in case of classified information spillage, without concern for the loss of the user's personal information.

The data-isolation technique allows for some of the controls on the hardware device to be relaxed. For instance, the camera and Bluetooth can be enabled for the user's personal activities. This personal use can be accommodated without compromising the protection of the sensitive information being processed on the mobile device. The tradeoff is that some functionality is then lost to the virtualized environment; pictures from the camera cannot be attached to emails from protected applications, for instance. Activation of application virtualization must not require additional user actions, nor permit user bypass of the isolation feature. Considerations should be given as to whether to allow tethering of GFE or non-GFE devices.

The substantial costs associated with this technique are similar to those of the fully managed solution. While the users may have additional features available to them for personal use, they won't retain possession of the information if the D/A must reclaim its hardware for any reason.

Though the D/A might not be able to manage the unmanaged portion of the device, the user's actions on that portion may still affect D/A systems, data, and operations. A mobile platform that is not updated and does not possess an up-to-date mobile security solution may still expose the D/A-managed container and information to increased risk through vectors such as covert channels. Illegal or unethical user actions on the unmanaged portion of the device can still open the D/A to liability. D/As should mitigate these risks through non-technical means, such as clear policies and strong training and awareness programs.

### User Furnished, D/A Partial Management

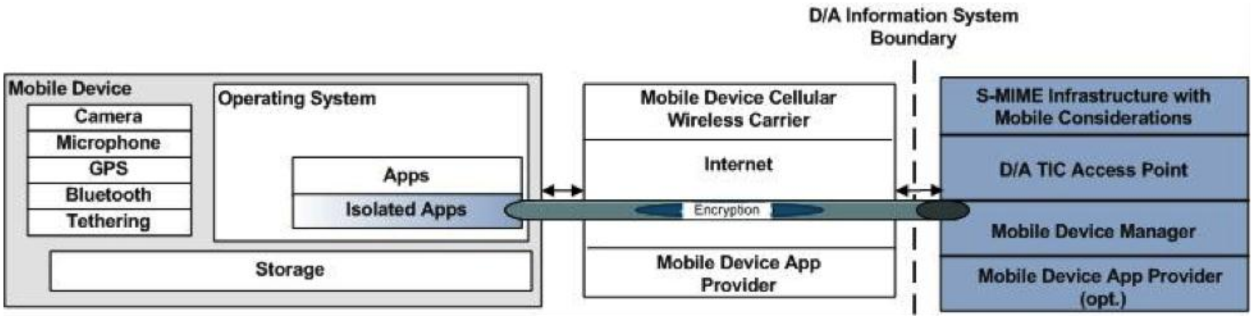
D/A Information System Boundary
Mobile Device
Camera
Microphone
GPS
Bluetooth
Tethering
Operating System
Apps
Isolated Apps
Storage
Mobile Device Cellular Wireless Carrier
Internet
Encryption
Mobile Device App Provider
S-MIME Infrastructure with Mobile Considerations
D/A TIC Access Point
Mobile Device Manager
Mobile Device App Provider (opt.)

*Figure 7: User Furnished, D/A Partial Management Use Case*

In this use case, shown in Figure 7, the D/A no longer controls the selection of the device, mobile service provider, operating system, or additional device features. The costs associated with managing these capabilities no longer fall to the D/A. This use case allows users to select the device that will best accommodate their needs and wants. Stipends or cost sharing for carrier coverage can be considered for users willing to use their personal devices for business activities. This use case assumes that the user will allow the device to be partially managed through a D/A MDM capability.

The D/A can specify minimum system requirements (e.g., the mobile device must not have been "rooted" or "jailbroken") and be able to enforce those requirements via the MDM capability. Policies for use can be limited to specific applications, where specific authentication techniques can be used. VPN capabilities may be allowed from non-GFE devices because the devices are enrolled in the D/A MDM. An MDM capability with broad device support is required since hardware, operating system, and application restrictions are relaxed for non-GFE devices.

Use of non-GFE devices for D/A work should be governed by a policy of informed consent with some technical enforcement:

- Monitoring and audit;
- Adherence to D/A-acceptable use policies while performing D/A work on the device; and
- Personal responsibility for the use of non-GFE device or loss of D/A data from theft or loss of the device (e.g., due to inadequate security configuration).

Although there is currently no legal precedent to do so, a D/A should work with their Office of the General Counsel (OGC) to determine if D/A policies or procedures could support the confiscation or destruction of Non-GFE equipment under specific circumstances, such as spillage of controlled unclassified information.

If the user's device supports the capability, the D/A may choose to implement a Dual-Persona scheme, similar to the GFE use case. For security assurance, activation of application virtualization must not require additional user actions nor permit user bypass of the isolation feature. The isolated environment created by the use of virtualization allows the D/A to manage encryption of data at rest and in transit, subject to FIPS standards. D/A security and management controls function only in the isolated space. This constraint allows the user full access to the device for other purposes, while maintaining D/A data security and application integrity. Remote wiping of isolated applications allows the user to retain personal information when the job assignment no longer requires the use of the mobile device for work-related activities.

The primary drawbacks of this implementation are the limited device types supported by the D/A MDM capability, and user reluctance to enroll a personal device in a business MDM system. If compromises in the isolated application are discovered, data exfiltration can occur with limited incident response capabilities available to the D/A.

Though the D/A might not be able to manage the unmanaged portion of the device, the user's actions on that portion may still affect D/A systems, data, and operations. A mobile platform that is not updated and does not possess an up-to-date mobile security solution may still expose the D/A-managed container and information to increased risk through vectors such as covert channels. D/As should mitigate these risks through non-technical means, such as strong training and awareness programs.

### User Furnished, Unmanaged Devices

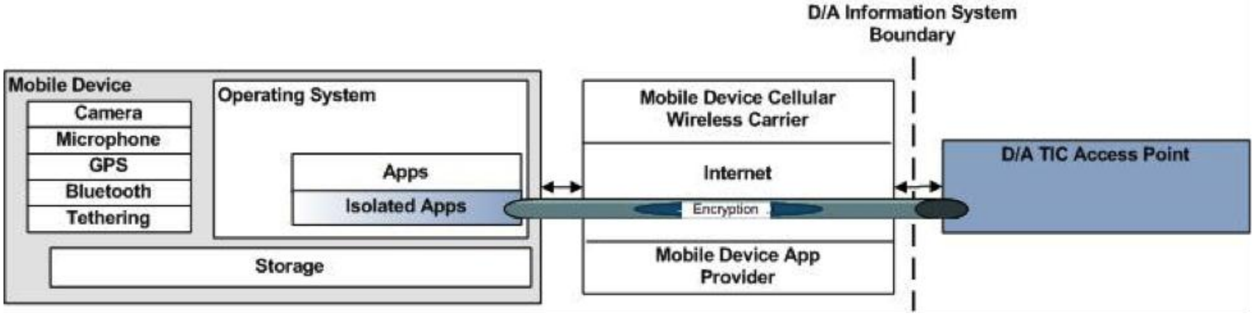

*Figure 8: User Furnished, Unmanaged Device Use Case*

In the case of unmanaged non-GFE mobile devices, as depicted in Figure 8, the D/A administrative domain is limited to the D/A telework infrastructure and externally accessible mobile application interfaces. The mobile devices are able to use clientless remote access capabilities, such as webmail, virtual applications, and visualization virtualization, but these devices have reduced business functionality. These remote access capabilities must be managed and accessed in a way that leaves little or no data on the mobile device including, for example, preventing a webmail client from downloading attachments.  Activation of application virtualization is impractical for this use case because the D/A is unable to manage security controls.

The D/A does not have any of the costs associated with the mobile device lifecycle and applies no restrictions to use of devices. Remote access capabilities may already be in place to support access from users' personal desktops, which can be enhanced to include access from mobile devices. D/As should prohibit the use of VPNs from non-GFE mobile devices, unless protections are in place to monitor traffic at the end point of the VPN connection. D/As can provide recommended device and carrier lists to users and may provide technical support when users employ these recommendations. User training on the safety, security, and use of mobile computing can also be provided.

Disadvantages of using an unmanaged implementation include greatly limited business functionality and the reluctance of users to use personal devices for business.

## 3.3 Sample Implementations

The sample implementations in this section represent only a few of the many possible implementation strategies. Each sample implementation is based on the reference architectures described in Section 3.1. These sample implementations are not meant to stand alone, and can be overlaid onto other implementations to form more complex mobile computing architectures.

### 3.3.1 Public Information Services

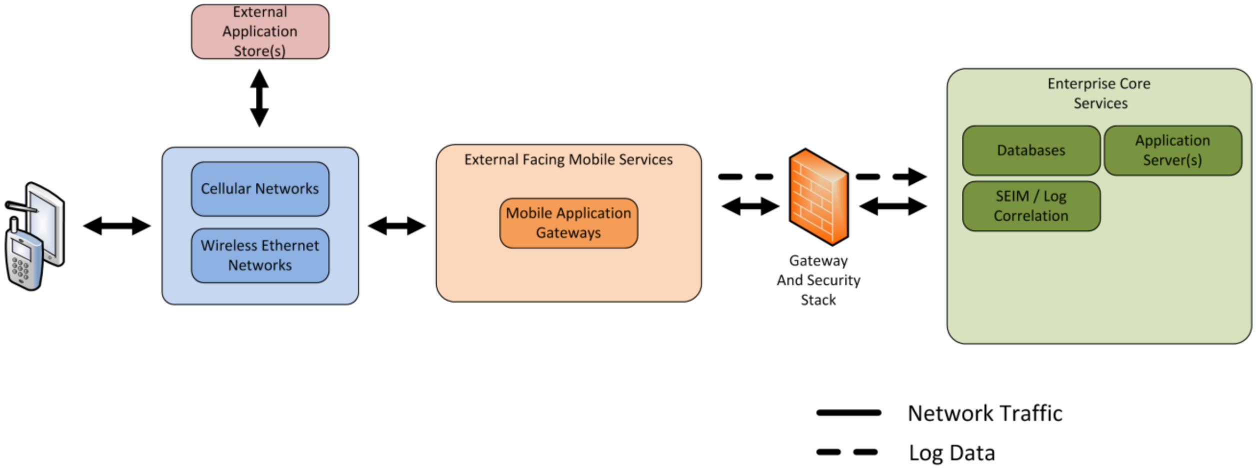
External Application Store(s)
Cellular Networks
Wireless Ethernet Networks
External Facing Mobile Services
Mobile Application Gateways
Gateway And Security Stack
Enterprise Core Services
Databases
Application Server(s)
SEIM / Log Correlation
Network Traffic
Log Data

*Figure 9: Public Information Service Implementation*

The purpose of this implementation, shown in Figure 9, is to provide public access to D/A data through a D/A-provided mobile application. Mobile application distribution is done through trusted third-party application stores. Mobile applications connect to D/A resources through the Mobile Application Gateway (MAG).

This configuration is by far the simplest and easiest to manage. The use of a firewall is unnecessary because the MAG only exposes the port(s) necessary to support the mobile application. Direct access to enterprise core services are prevented by the network gateway and security stack, allowing only traffic from the MAG to pass through. All traffic from the MAG to the enterprise core is still inspected by the security stack.

Example Benefits of the Public Information Service Implementation:

- Simple management and configuration;
- Low or no-cost distribution of client mobile applications; and
- Minimal network exposure to attacks.

Example Drawbacks of the Public Information Service Implementation:

- External users of a D/A provided mobile service can generate support requests to the D/A which may increase load on D/A IT resources; and
- Increased possibility of cloned/malicious client applications being created and distributed because of the use of third-party application stores.

### 3.3.2 Remote Data Entry

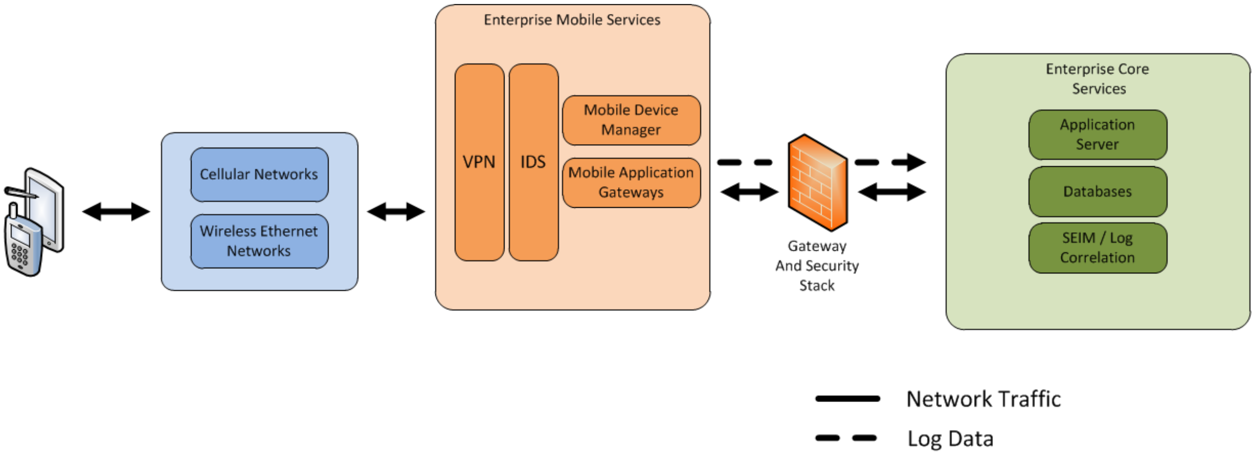

*Figure 10: Remote Data Entry Implementation*

The purpose of this implementation, shown in Figure 10, is to provide a pool of devices that D/A employees can check out to perform data entry at remote, non-D/A sites. The D/A uses a Mobile Device Manager to provision a pool of mobile devices that are assigned to employees for temporary use. All mobile devices connect to D/A mobile services through a Virtual Private Network (VPN), which minimizes the public-facing network exposure of mobile services. Mobile applications connect to D/A resources through the Mobile Application Gateway.

Although devices are D/A configured and managed, the possibility exists of a zero-day exploit or other mechanism that would compromise the mobile devices. An intrusion detection system is placed between the VPN and mobile services to monitor network traffic to detect potential malicious network traffic. The network gateway and security stack is configured to allow traffic only to and from the MDM and MAG to pass.

Lost or stolen devices can be wiped or located (if GPS enabled) by the use of the MDM.

Example Benefits of the Remote Data Entry Implementation:

- Simplified configuration management of mobile devices;
- Simple, highly regulated access to D/A data sources; and
- Mobile computing infrastructure with minimal surface area for attack.

Example Drawbacks of the Remote Data Entry Implementation:

- A large number of client devices that are not tied to a specific user, limiting attribution;
- Increased D/A costs to provide mobile devices; and
- Increased D/A costs to provide end-user support for mobile devices.

### 3.3.3 Government-Furnished Mobile Devices, Fully Managed

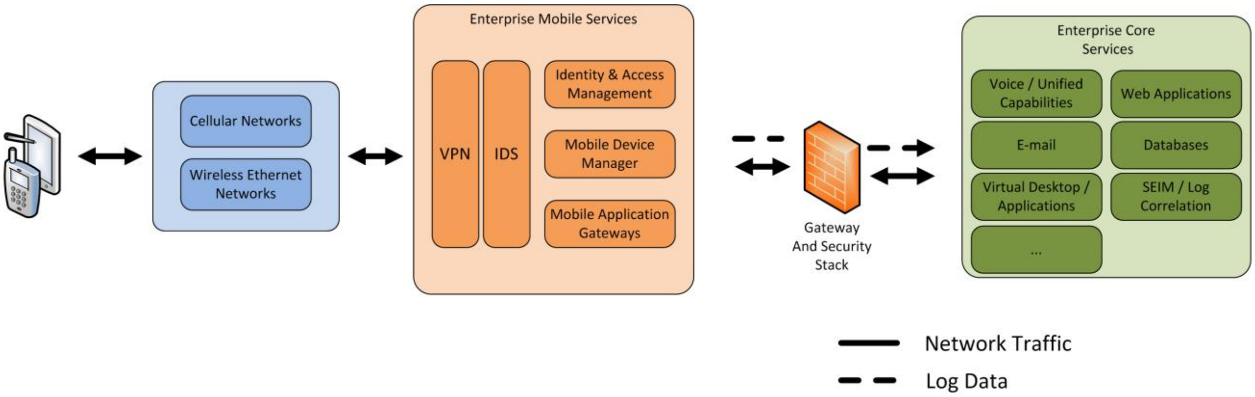
Cellular Networks
Wireless Ethernet Networks
Enterprise Mobile Services
VPN
IDS
Identity & Access Management
Mobile Device Manager
Mobile Application Gateways
Gateway And Security Stack
Enterprise Core Services
Voice / Unified Capabilities
Web Applications
E-mail
Databases
Virtual Desktop / Applications
SEIM / Log Correlation
...
Network Traffic
Log Data

*Figure 11: GFE, Fully Managed Implementation*

This implementation, shown in Figure 11, represents a basic D/A implementation of a GFE solution with no expectation of personal use of the mobile devices. In this implementation, the D/A is responsible for furnishing one or more mobile computing devices to employees who are allowed mobile access. The configuration of all devices is managed by the D/A through the use of a mobile device manager that uses the Identity Manager to federate device user identities with the enterprise authentication mechanism. The federated identities are used to identify which mobile device profile is enabled on a mobile device, allowing the D/A to create different profiles based on a user's role in the D/A.

Applications are pre-loaded on all devices and managed by the MDM. This centralized approach allows the D/A to ensure that all devices are using the same version of the application, eliminating the costs associated with supporting multiple versions. Use of FIPS-compliant device storage encryption is also activated and mandated through the MDM configuration policy. Finally, lost or stolen units can be wiped as necessary through use of the MDM.

Although the D/A has full control over the devices, access to mobile services is still protected by the use of an intrusion detection system and mobile application gateway. The use of a FIPS-compliant VPN solution enables remote access to D/A mobile application resources.

Example Benefits of a Government-Furnished, Fully Managed Solution:

- Reduced support costs due to standardized hardware and software;
- Integration of mobile device user identities with enterprise identities, simplifying profile management and providing attribution;
- Use of IAM and MDM, which allows each user to have multiple devices, each using the same profile;
- Support for multiple types of users with separate use cases for each; and
- Use of a VPN, which provides minimal public network surface area for attack.

Example Drawbacks of a Government-Furnished, Fully Managed Solution:

- Increased D/A costs to provide mobile devices;
- Increased D/A costs to provide end-user support for mobile devices;
- Increased IT overhead to implement and maintain multiple mobile user profiles;
- Increased complexity of the MDM;
- Use of federated identities, which increases the severity of credential theft, and increases the attack surface for credential theft; and
- Possible use of a dual-connected device (VPN/cellular) as a bridge into the mobile space as an avenue for attack.

### 3.3.4 Government-Furnished and Managed, Personal-Use Enabled

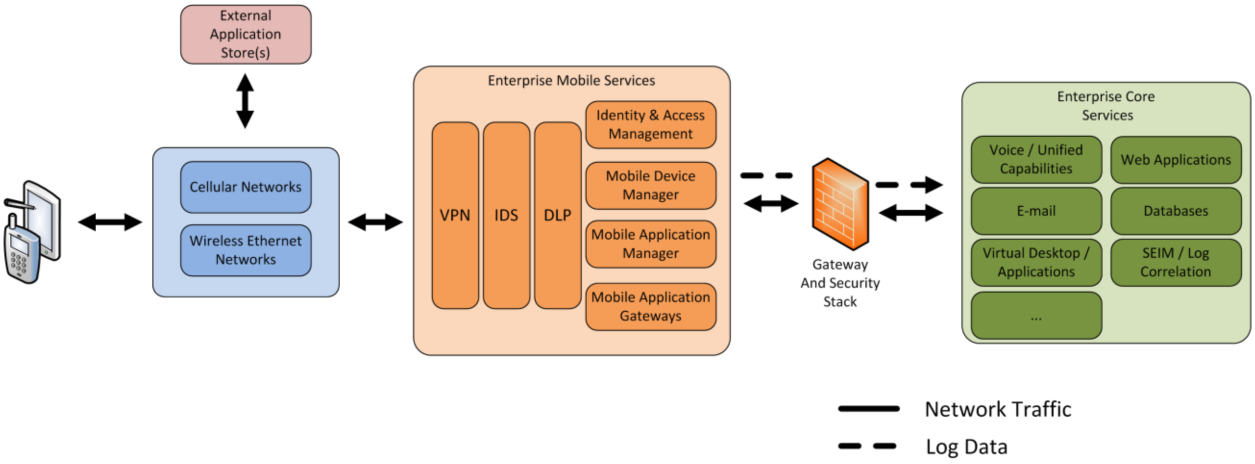
External Application Store(s)
Cellular Networks
Wireless Ethernet Networks
Enterprise Mobile Services
VPN
IDS
DLP
Identity & Access Management
Mobile Device Manager
Mobile Application Manager
Mobile Application Gateways
Gateway And Security Stack
Enterprise Core Services
Voice / Unified Capabilities
Web Applications
E-mail
Databases
Virtual Desktop / Applications
SEIM / Log Correlation
...
Network Traffic
Log Data

*Figure 12: GFE Managed, Personal-Use Enabled Implementation*

This implementation, shown in Figure 12, is based on the use of a Dual Persona enabled mobile device that is provided to a user by the D/A. Although similar in nature to the GFE Fully Managed implementation, this implementation adds the use of a Mobile Application Manager to manage the creation and use of a protected application space (i.e., container) on the mobile device. All other government provided applications are installed and managed by the MDM. This use of containers is discussed in the Government Manager, Dual Persona mobile device use case. The MDM is used to configure the base device, including the use of FIPS-compliant storage encryption.

Because all D/A-critical applications, including the VPN client, are expected to run within the isolated environment, access to third-party application stores is enabled. This approach allows users to personalize its device, but not to place agency data at risk. The use of an MDM allows the D/A to blacklist specific applications known to be harmful or dangerous, even if they are installed from a third-party application store. This behavior may be dependent on the specific implementation of the MDM.

Federated identities can be used to define the size, contents, and potential interactions of the protected container with the host device, as well as to specify the contents of the protected container.

Since the VPN client resides within the protected container, applications running outside the container have no access to internal D/A mobile services. This separation provides an added layer of protection to the solution and limits the effectiveness of zero-day attacks against the mobile infrastructure.

As in the previous implementations, an IDS is used to monitor and protect the mobile infrastructure and access to D/A resources is regulated by the Mobile Application Gateway. The MDM can be used to wipe the whole mobile device, or just the protected container, as necessary.

### Example Benefits of the GFE, Personal-Use Enabled Implementation:

- Greater flexibility for mobile computing devices;
- Protected containers allowing personal use, while minimizing exposure of D/A data;
- Use of VPN inside the protected container that limits the utility of the mobile device as an attack bridge into the mobile device infrastructure; and
- Smaller chance of credential compromise because credentials are used only in the protected container.

### Example Drawbacks of the GFE, Personal-Use Enabled Implementation:

- Use of a protected container that may limit the utility of some applications;
- Increased management complexity;
- Increased support costs due to possible high number of application configurations;
- Increased costs associated with providing devices to users; and
- Uncertain/undetermined legal implications for users and their personal data.

# 4. Mobile Security Functions

This section presents a brief description of the security functions and a summary of mobile-infrastructure-related characteristics for each security function needed to manage mobile devices and their supporting infrastructure. These mobile-infrastructure-specific characteristics are not new requirements; they are highlights of existing guidance and standards set forth in NIST publications, GAO reports, Committee on National Security Systems (CNSS) policy, Federal laws, industry standards, and best-practice guidelines. General technical descriptions of security functions and their application in externally connected networks are described in great detail in the Trusted Internet Connection (TIC) Reference Architecture v2[7].

Security functions are the building blocks for mobile infrastructure security. Unless specifically noted, all security functions are mandatory for mobile infrastructures. Agencies ensure that these security functions are incorporated into their security policies and practices. The controls presented in this document are derived from the TIC reference architecture v2 security controls, which are, in turn, derived from security controls and associated guidelines described in NIST Special Publication 800-53[8] in accordance with FISMA, OMB, and other Federal requirements. In most cases, the controls described are tailored specifically for mobile architectures, but still conform to the more general case.

## 4.1 Personnel and Facilities Management

The management security function includes the processes for assessing and managing an information processing system and the risks associated with that system. Mobile-infrastructure-specific characteristics include the following:

- The agency develops, documents, and implements security policies that identify which users are authorized to connect wirelessly to an organization's networks and the types of information allowed to be transmitted across wireless networks.
- The agency performs risk assessments to understand mobile infrastructure threats, the likelihood that those threats will be realized, and the potential impact of realized threats on the value of assets.
- The agency ensures resource adequacy in the following ways:
  - Maintain a staff of cleared personnel with current credentials and adequate training to manage a mobile infrastructure and provide mechanisms to revoke their credentials upon termination. The revocation mechanism should include the ability to adjudicate

[7] https://max.omb.gov/community/download/attachments/327058467/TIC_Reference_Architecture_v2_Final_2011-09-01.pdf?version=1&modificationDate=1314983111449.

[8] NIST Special Publication 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems*, August 2009.

revocations associated with staff transfers, access agreements with other D/As, and third-party security personnel.

  - Sustain a level of funds to adequately operate and maintain mobile capabilities in accordance with applicable policy.

- A configuration baseline is established that defines the minimum requirements for compliance with policy, and ensures that mobile infrastructure hardware, firmware, software, and documentation are adequate to protect the mobile infrastructure.
- The agency designates a personnel position or organizational entity to track mobile infrastructure product vulnerabilities and wireless security trends to ensure continued secure implementation of the mobile infrastructure.

The following NIST SP 800-53 Revision 4 security control families support this security function: Access Control (AC), Configuration Management (CM), Program Management (PM), Personnel Security (PS), and Risk Assessment (RA).

### 4.1.1 Training

The training process addresses the need for network administrators to have sufficient training to administer a particular class of network and the need for users to be educated about network-specific security issues. Training is required for every network administrator and user. Mobile infrastructure administrators need sufficient training to design, operate, and maintain mobile infrastructures. User training about mobile infrastructure security issues provides awareness of risks associated with mobile infrastructure technologies. The training security function is supported by the policies and procedures developed under the management security function.

Mobile-infrastructure-specific characteristics include the following:

- Mobile infrastructure security training is part of the agency's overall security training program. Managers, technical support personnel, and users of mobile technologies are educated about the risks of mobile technology and how to mitigate those risks before they can be authorized to operate in the mobile infrastructure.
- Mobile security training for users includes mobile security awareness, policy overview, and best practice guidelines for the following:
  - maintaining physical control of mobile devices;
  - protecting sensitive data on mobile devices with encryption;
  - disabling wireless interfaces on mobile devices when not needed;
  - reporting lost or stolen mobile devices promptly;
  - using policies on agency and non-agency networks; and
  - properly managing passwords.

- Mobile security training for managers and technical support personnel addresses all mobile infrastructure components and includes all user-specific security training in addition to education in the following areas:
  - security risks associated with choosing one authentication or encryption method over another among the FIPS 140-2 approved methods;
  - security requirements for the mobile infrastructure, including but not limited to security measures for data at rest, data in transit, privacy and legal constraints, and a password policy; and
  - rules, procedures, and restrictions for the use of social media.

- Mobile environment training for all personnel includes security awareness training about the risks of using unauthorized mobile client devices and applications.

### 4.1.2 Physical Controls

The physical controls security function specifies facility, physical security, and facility management standards that are necessary to ensure the physical security and operational resiliency of the mobile infrastructure.

Many of the characteristics associated with physical controls of a wired LAN, WAN, wireless LAN, and telework infrastructure apply to a mobile infrastructure. Mobile infrastructure-specific characteristics include the following:

- A physical security plan is provided to ensure that all components of the mobile infrastructure are securely installed and can be accessed only by authorized personnel. Additionally, the physical security plan provides policies for physical control of users' mobile devices.
- The inherent nature of the devices that manage the Mobile infrastructure can be divided into two components categories:
  - Core: This category contains infrastructure components such as MDM, IAM, MAM, and WiFi access point controllers, as well as the peripheral systems that support Mobile services. These components are critical to the mobile infrastructure and should be located in a secure facility[9] (such as a data center) and architected to be resilient to physical threats from both individuals and environment.
  - Edge: This category contains components (e.g., WiFi access points) that are close in proximity to the end-user Mobile device whose purpose is to provide secure layer 2 and 3 transport of the data, service, diagnostic and control planes[10] of the Mobile service infrastructure back to the core components. While the capabilities of edge

[9] The NIST SP 800-53 Revision 4 Security Control Families Support this Security Function: Physical and Environmental Protection (PE).

[10] Please see Appendix E, Glossary, for a definition of "control plane."

infrastructure components are extremely narrow, all enterprise scale Mobile infrastructures require core management components for edge components to function at all. Since edge components are close to the end-user device they are generally in insecure areas. However, as their capability is extremely low and they house no assets-at-rest their compromise generally poses a low security risk. With respect to managing these edge components, some vendors have implemented management features and strategies that detect if edge components have been taken off line temporarily or have their connectivity interrupted for a specific period of time and automatically scan and reconfigure them to insure compliance to the management policy.

## 4.2 Identity and Access Management

Authentication is the process of verifying the identity of a user, process, or device.[11] Agencies uniquely identify and authenticate network users and client devices for access to the D/A network and resources. A mobile infrastructure may use the same authentication methods as the core agency network, or it may use its own authentication schema. Only credentialed users and devices that are authenticated via mobile infrastructure authentication servers are granted access to internal enterprise resources.

Multiple authentication layers exist in a mobile device and most are not integrated across administrative or technology domains, but MDM solutions greatly help to configure and enforce the layers. This security function is provided primarily by IAM, as well as the MDM and MAM components. Some examples include the following:

- Physical device UI: via a password (MDM, IAM);
- Syncing service: to USB, generally via a unique MAC address (MDM);
- Carrier: WAN, MMS/SMS, cellular, cloud application or storage services (MDM);
- Bluetooth: via a unique MAC address and/or simple shared secret (MDM);
- Local application: via a local password (MAM);
- Wi-Fi: via a shared secret and/or MAC address (MDM, IAM);
- VPN: via a shared secret, PKI, or two-factor authentication (IAM, MDM);
- Remote service, network or application: via smartcard implementation of Homeland Security Presidential Directive 12 (HSPD-12) over NFC[12] (MDM, IAM);
- Remote application: via a shared secret, PKI, or two-factor authentication (MDM, IAM); and
- Remote virtualization and/or sandbox infrastructure: via a shared secret, Public Key Infrastructure (PKI), or two-factor authentication (MDM, IAM, MAM).

Some functions of the MDM, IAM, and MAM overlap depending on vendor implementations.

[11] NIST Special Publication 800-63, Electronic Authentication Guideline.

[12] NIST, FIPS 201-2 and Derived Credentials, Ferraiolo H., February 1, 2012, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_der_cred_ferraiolo_h_fips_201-2.pdf.

### 4.2.1 Identity and Access Management Mechanisms

Many of the mechanisms associated with authentication in a wired LAN, wireless LAN, and telework infrastructure apply to a mobile infrastructure. Mobile-infrastructure-specific mechanisms include the following:

- While traditional authentication mechanisms that are password based can be circumvented, there are multi-factor technologies that provide a stronger identity coefficient to the end user. The D/A should "right-size" multi-factor technology functionality with the criticality of the asset it is protecting with the use-case requirements of the end user and the D/A's asset use policies.
- The agency's PKI certificate policy, certification practice statement, and related processes are revised to support the mobile solution (e.g., revise the agency's PKI certificate policy to include the new mobile certificates, maintain certificate revocation lists by including mobile certificates).
- HSPD-12 was initiated to address wide variations in the quality and security of identification used to gain access to secure facilities. As stated in the objective statement, "in order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a Federal standard for secure and reliable forms of identification."[13, 14]

NIST is in the process of finalizing FIPS 201-2 which is the technical standard for HSPD-12. NIST has been considering architectures (some options consider using Near Field Communication (NFC)) for integrating the smartcard capabilities with mobile devices based on use cases of Federal employees.

The following NIST SP 800-53 Revision 4 security control families support this security function: Identification and Authentication (IA) and Access Control (AC).

### 4.2.2 Authorization

All users are neither required to have the same access and functional capabilities in a mobile environment, nor access to the same, specific digital assets. Considerations are given in the following areas of the mobile device architecture to restrict user access and functional capabilities:

- What the user can do on the device (e.g., configure, install);
- What the user has access to with respect to D/A data assets and the applications that access them; and

[13] Homeland Security Presidential Directive-12 (HSPD-12), http://www.dhs.gov/homeland-security-presidential-directive-12.

[14] OMB M-05-24, www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf.

- What the user has access to within the mobile device management infrastructure (e.g., configuration, device management, monitoring).

While there are many vendor offerings and technologies in both the identity and authorization management domains, almost all dovetail with existing MDM environments, which makes it possible to provision user capabilities appropriately.

### 4.2.3 Network Access Control

Network Access Control (NAC) is a methodology with mature standards where an end host authenticates with the network prior to being able to use its services. It also tries to combine end-host configuration verification services (e.g., vulnerability assessment, patch management, antivirus, IDS/IPS, firewall) prior to network access credentials being given. For example, if an end host does not meet specific configuration verification policies, the device may be given access to a portion of the network where the services are greatly reduced, but the host can still remediate the policies that it was in violation of (e.g., patching) then try to gain access again when the actions have been successfully completed. This process is called “sandboxing” or “quarantining.”

There are very mature and widely adopted standards and methods (e.g., 802.11X) for LAN devices, and most of the major OS vendors in the personal computer domain include them in their new releases. In the mobile device domain, this technology is maturing rapidly because there are multiple vendors that are highly integrated with the MDM that offer both agent and agentless solutions. The constraints for WAN and wireless access are different from LAN access; WAN access has performance limitations, specifically over WiFi, but especially over cellular networks. Obviously, these limitations can increase the time it takes for the NAC service to validate the device.

## 4.3 Data Security

Data management is one of most critical mechanisms used in managing a mobile device infrastructure. This topic has a wide range of subcategories, such as:

- Digital Asset Protection
  - Asset Access: the management of direct access to digital assets of the D/A and the applications that shepherd them;
  - Data at Rest (DAR): the end-to-end management of data as it resides in different parts of the infrastructure and on different devices and technologies;
  - Data in Transit (DIT): the management of data as it travels from the source of the asset to the end device; and
  - Disposal: the disposal requirements for mobile infrastructure components.
- Diagnostic Data Management (DDM): the management of any diagnostic data that aids in the processes of infrastructure management, diagnostics, forensics, and the identification of both normal behavior and anomalies of the mobile infrastructure.

### 4.3.1 Digital Asset Protection

As with traditional personal computing devices, carefully consider the protection of digital assets no matter where they exist. Mobile devices are much more susceptible to vulnerabilities and attacks because of their level of technical (e.g., OS, hardware capabilities, applications) maturity compared to older more mature and powerful devices with greatly increased computational resources. Also, because of their size, mobile devices are more easily lost or stolen.

Prior to beginning a mobile initiative, we recommend that the D/A complete a digital asset definition and management process[15] that helps to assign metrics to digital assets to better assess how the assets should be administered. This process serves as the basis for an end-to-end mobile data architecture that defines a number of asset attributes by posing a series of questions:

- Who has access to what data?
- What identity levels are needed?
- What actions can users take on the data?
- Where and when do users have access?
- What types of devices can have access?
- In what physical locations can the devices be used?
- Are specific locations unsuitable to access D/A data from?
- Are there availability metrics that define the quality of access?
- Where can the data exist from its native source and how is integrity and confidentially assured?
- Should the change log be retained?
- Does the data have to be encrypted at rest (if allowed) or in transit?
- Why is the presentation format of the data (e.g., raw, PDF) viewable only through a UI application presentation layer?

These attributes define the data access policies, which, in turn, build the requirements for the mobile device architecture. Possible products, technologies, and methods that will be key components in the mobile architecture include the following:

- *Mobile Device Managers (MDMs)* that manage the configuration and monitor the end device;
- *VPN* that ensures user identity and provides data-in-transit encryption;
- *Application Proxies* that assemble the data for analysis or presentation;
- *IDS/IPS* that provide alerts, reporting, and defense against possible intrusions;
- *SIEM/Flow/Packet Capture* that provides an event orchestration framework and application environment for forensics and security analytics;
- *Identity and Access Management Systems* that provide authorization and authentication;

[15] SEI Publication, CERT Resilience Management Model Version 1.0, May 2010.

- *Sandboxed Mobile Environments* that ensure that data at rest on the mobile device is compartmentalized from the OS, its subsystems, and other applications;
- *Virtual Desktops* that are required when data does not rest on the mobile device and are displayed (e.g., of some flavor of OS or presentation application) such that the data is exposed only while it resides on the "far end," within the D/A's infrastructure; and
- *Data Encryption* that ensures that data at rest on the mobile device is encrypted if the device is lost, stolen, or compromised.

If a virtual desktop or sandbox environment is used and managed via the MDM we suggest, the following policies are recommended:

- All virtual desktop and sandbox environments must conform to the same agency IT data storage security policies and requirements as laptop environments. In addition, ensure that mobile applications do not impinge on D/A data storage security policies;
- If possible, perform conformance testing to ensure data isolation between the native OS platform and the virtualization and/or sandbox environment; and
- Verify that specific storage configuration parameters of the mobile device can have its attributes managed remotely, and possibly isolated from the user's control, or, in some instances, their view.

The following NIST SP 800-53 Revision 4 security control families support this security function: Audit and Accountability (AU), Configuration Management (CM), Media Protection (MP) and System and Communications Protection (SC).

Upon the end-of-life or retirement of a mobile device, consider removal of the device's access to the D/A infrastructure via the MDM, and removing D/A asset data and user personal data from the device. Depending on the OS, the completeness with which data and digital artifacts can be removed varies. Check with the OS manufacturer to verify the completeness of the process. There also may be digital artifacts that exist in the cell provider's infrastructure. A D/A should develop comprehensive sanitization policies and processes for all mobile devices and infrastructure components.

### 4.3.2 Diagnostic Data Management (DDM)

DDM is necessary to store logs collected as part of the logging security function and data collected as part of the intrusion detection and prevention security function. Many of the characteristics associated with data storage in a wired LAN, wireless LAN, and telework infrastructure apply to a mobile infrastructure. Mobile-infrastructure-specific characteristics include the following:

- Mobile infrastructure diagnostic (e.g., configuration, security, application, system, call) audit records (mostly in the form of log files) should be transferred to the mobile infrastructure diagnostic and log collection system as near real time as possible and, if not, should be securely stored for later transmission.[16] After transfer, the data should be deleted from the device. Any diagnostic log records generated by the MDM should be managed as if they are a highly critical service vital to the enterprise. Members of the technical staff who have access to these records have an added responsibility since these records could correlate specific events to the behavior of the user who owns the device. Depending on the MDM and its configuration, the diagnostic log records may be extremely sensitive in nature.

- Establish a diagnostic log or audit record retention policy to meet legal, compliance, and other D/A requirements when disposing of a mobile infrastructure component.

## 4.4 Device Management

Probably the most critical process of mobile end-device security is their management. This management includes not only the configuration of their OS and applications, but also software patches, their A/V, IDS/IPS, and digital asset data management systems, such as a "sandbox" or "virtual desktop." The management process is accomplished by a mobile device manager. There are a wide variety of vendors for all the major classes of mobile devices that offer solutions with broad feature offerings that are highly integrated into the mobile device. MDMs also have high value in providing granular management capability for BYOD devices for which the required management of the end device may be restricted by D/A policies. The MDM is also highly integrated into the identity, authorization, and network access control systems.

### 4.4.1 Host Security

While network-based security is highly valuable, end devices move between networks that have varying capabilities, management, access, and acceptable use policies. Even on a trusted network, the end host should have the same level of security assertiveness in protecting itself from external attack vectors as it would on a non-trusted network. Consider internal attack vectors in which a "suspect" application could have access to both sensitive data and configuration settings. Therefore, the end mobile computing device must adhere to good host management policies and practices. The following are major areas of focus that should be given attention:

- OS and Application Patching;
- Configuration Management;
  - OS
  - applications, both functional and the data they have access to
  - data segmentation framework (i.e., sandbox and virtual desktops)
  - network access, both egress and ingress, if possible, on all network interfaces (WiFi and cellular)
- Security Frameworks (capability dependent on the OS platform of the device);

[16] NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.

  - antivirus
  - firewall
  - auditing and monitoring.

Most of the areas mentioned can be managed via the device's MDM service, including the capabilities of the MDM and the native device OS. Any actions the MDM takes to manage these areas, such as system events (i.e., both faults and acknowledgements of a successful action), should be sent to the logging and diagnostic infrastructure to assist in end-device behavior validation and forensic processes if needed.

### 4.4.2 Configuration

The configuration security function describes the appropriate logical and physical configuration settings that are necessary to deploy and maintain a secure mobile infrastructure, including its component devices.

It is essential that D/A infrastructure teams invest time in carefully choosing an MDM solution that enables the discovery, management, and enforcement of D/A policies that are driven by D/A use cases compiled from the users themselves, not just from the IT implementation team. Plan to conduct a pilot program that stresses the mobile device and its supporting infrastructure, including the MDM. Presently, the technology is advancing at a breakneck pace, so it is critical that any MDM solution be able to scale to a number of different mobile device vendors, adapt to different device features, accommodate essential third-party apps, and dovetail into the TIC architecture.

Mobile infrastructure characteristics, which integrate with the MDM as a management, discovery, and enforcement vehicle, should include the following:

- Configuration guidelines must be developed for mobile infrastructure devices and networks that define minimum requirements for hardware, firmware, software, and documentation.[17] Ensure that configuration controls exist to govern regular software patches and upgrades. An MDM solution can be used to discover devices that are not sufficiently current in their configuration, firmware, or application patches, and either disable them (i.e., wipe clean or render them useless) or force an update. In addition, policies must include guidance on implementing patches and updates.
- All cryptographic elements of a mobile infrastructure must be FIPS validated and must follow agency policies with regard to key material storage, rotation, and destruction.
- Vendor and default user accounts and passwords must be changed before the mobile infrastructure is brought online.

[17] NIST Special Publication 800-124, Guidelines on Cell Phone and PDA Security.

- Administrative access to mobile infrastructure devices must use multi-factor authentication in accordance with Government-wide policy.[18,19]
- When procuring and configuring agency-issued mobile devices, the following guidelines must be observed:
  - Agency-issued mobile devices must use authorized mobile methods only, have enabled firewalls (IP, MMS/SMS and Bluetooth),[20] have all unnecessary features disabled, and enable features designed to prevent malicious software from executing on the device.
  - Filters should be employed to limit which applications have access to specific device resources, such as the microphone, geo-location service, or other applications such as the address book.
  - Operating system and application security configuration guidelines are established for agency-issued mobile devices.
  - Audit changes in configuration controls through continuous monitoring techniques and transfer audit records from the mobile device to the MDM as quickly as possible. Near real time or periodic auditing is possible when a device has network connectivity, but audit information must be queued for transfer when connectivity is not possible. When there is no connectivity, audit information must be queued for transfer and then removed from the device.
- Policy-based filtering must be enforced to restrict the download of new applications to only specific applications through preapproved application stores.
- When disposing of a mobile infrastructure component, all sensitive configuration information, including data stored on the devices and passwords, must be removed.
- Manage a “poison pill” application that renders the mobile device partially or completely useless based on a predefined use and behavior monitoring and auditing policy.

The following NIST SP 800-53 Revision 4 security control families support this security function: Access Control (AC), Configuration Management (CM), Identification and Authentication (IA), Media Protection (MP), Personnel Security (PS), System and Service Acquisition (SA), System and Communications Protection (SC), and System and Information Integrity (SI).

### 4.4.3 Software Validation and Patch Management

As with traditional personal computational computing devices, software validation and patch management is an essential part of the device manage framework. The mobile device strategy should dovetail with the existing personal computing device strategy.

[18] OMB Memorandum 11-11, FIPS PUB 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

[19] NIST Special Publication 800-63, Electronic Authentication Guideline.

[20] NIST Special Publication, 800-121, Guide to Bluetooth Security (draft).

The MDM is typically the primary mechanism for software validation and patch management. Additional software validation may be performed during acceptance testing of enterprise applications to be managed through the MDM, or to be made available through a D/A MAS. The capabilities and functionality of the MDM varies greatly depending on the device managed (and the OS version) as well as the vendor of the MDM.

An additional complexity with mobile devices is that some “app stores” may have software that does not conform to the policy of the D/A for a number of reasons. There are multiple mitigation strategies that include restricting access to the “app store,” restricting what applications (and versions) can be downloaded, and building an enterprise “app store” within the D/A infrastructure that includes only approved, validated, and tested applications.

If the D/A builds its own custom applications, it should ensure that secure software engineering practices are followed. Also, some third-party software validation services ensure that custom applications are engineered appropriately via code reviews and penetration techniques.

## 4.5 Secure Communications

The secure communications security function secures administratively supported communications from unauthorized access, disclosure, and modification. A secure communication protocol is required to appropriately protect confidentiality, authentication, and content integrity. Communications can be secured via encryption through network VPN (hardware or software based) at the data or network layer of the ISO stack or through the application itself. Agencies follow Federal encryption standards to protect agency data during user access to information systems.[21]

Mobile infrastructure communication characteristics include the following:

- Administration and network management of mobile infrastructure equipment use strong multi-factor authentication and encryption for all communications;[22]
- All cryptographic elements of a mobile infrastructure must be FIPS validated, and must follow agency policies with regard to key material storage, rotation, and destruction. The MDM must enforce, manage, and monitor the policies;
- Whether from malicious jamming, equipment damage, or extreme loading due to an extraordinary event, the cellular network can become congested, rendering denial of access to enterprise services and communications in general. The D/A should consider the application of National Security/Emergency Preparedness priority services as part of its threat mitigation strategy; and
- Encrypt network communications channels to protect data in transit and use application-based encryption to protect digital assets over both non-encrypted network communication channels

[21] FIPS PUB 140-3 (Revised DRAFT 09/11/09) Security Requirements for Cryptographic Modules.
[22] NIST Special Publication 800-46, Guide to Enterprise Telework and Remote Access Security.

and, if possible, data-at-rest. The data encryption on the device is highly dependent on the application or a "sandboxed" infrastructure.

The following NIST SP 800-53 Revision 4 security control families support this security function: Access Control (AC), Audit and Accountability (AU), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), and System and Communications Protection (SC).

## 4.6 Continuous Monitoring and Auditing

Distributed system monitoring and auditing are core processes essential to maintaining situational awareness of critical mobile device infrastructures domains (e.g., network, system, application, security, authorization/authentication, environmental). These processes can provide near-real-time diagnostic and forensic capabilities for the detection of and visibility into anomalies. They can also shed light on deviations from normal baseline behavior or suspicious activities, as well as verify the implementation of corrective actions. Monitoring and auditing processes also provide a foundation for capacity planning and ensure a reliable source of data for SIEM infrastructures, which are the "sensory network" for the security analysis of anomalies.

Note that monitoring and auditing supports the required set of security controls, under the NIST security controls, continuous monitoring (CM-7)[23].

Monitoring and auditing infrastructures are essentially the diagnostic data management infrastructure. It is essential to monitor and audit not only the service and data planes of the mobile device infrastructure, but also the control plane. If the control plane is compromised, an organization could become highly vulnerable to exploitation with little or no detection by bypassing key monitoring processes through reconfiguration of the infrastructure.

A system audit is a periodic evaluation of security. Monitoring is an ongoing review of the behavior of distributed infrastructures and their users in near real time (if possible). Security auditing of near-real-time diagnostic data, for example network performance of a key LAN, can indirectly be a good bellwether of an intrusion. A mobile infrastructure security assessment includes end-to-end operational verification of mobile client device services, configuration settings, audit logs, and relevant diagnostic information. Monitoring and auditing security, integrated with logging infrastructure, supports the data storage security functions, and, in turn, complements the traffic inspection and content filtering security functions.

When an organization adopts a continuous monitoring strategy the following are the major areas of focus which provide high value by establishing a behavioral baseline for the availability, accessibility, confidentially, integrity and retention attributes of the assets (e.g., the organizations data and its supporting infrastructure) of an organization:

[23] NIST Special Publication 800-53 Rev 4, CA-7, page F-60.

- The management of the end-user and infrastructure components, which include changes in the software and hardware inventory, configuration management events;
- Understanding the security impact of changes to the infrastructure by establishing situational awareness through the analysis of its behavior both the operational faults and acknowledgment of successful events in the network, system, application, security and environmental domains;
- Providing continuous security control assessments that verify the operational policies of the assets and the infrastructure that shepherd their use; and
- Exposes the event horizon of the homeostasis of the organization's mobile infrastructure and exposes anomalies of both quiescent and new potential threats as well as vulnerabilities.

Mobile infrastructure-specific continuous monitoring and auditing characteristics include the following:

- Mobile infrastructure security audit processes and procedures are developed. Mobile infrastructure security assessments are performed regularly (e.g.  hourly, daily, weekly, monthly or quarterly) with additional assessments at random intervals to ensure that mobile infrastructure security requirements are met;
- Authorized mobile client devices are audited periodically to ensure that they meet security configuration requirements, including authentication mechanisms, data encryption, and administrative access;
- Audit logs are reviewed frequently as policies dictate. Auditing tools can be employed to automate the review of audit data;
- Retention period policy for the audit data is defined; and
- Tight integration is maintained within the mobile device infrastructure, including application management, configuration management, and device management.

This information is used to improve security of the mobile infrastructure by:

- Detecting unauthorized devices;
- Identifying operational anomalies and behaviors of a device or portion of the supporting; infrastructure that deviate from a predetermined baseline;
- Verifying that devices are agency-authorized devices;
- Identifying security or operational configuration change anomalies or violations; and
- Monitoring and auditing the configuration and behavior, as well as the use of the device.

The following NIST SP 800-53 Revision 4 security control families support this security function: Audit and Accountability (AU) Configuration Management (CM) and Identification and Authentication (IA).

### 4.6.1 Traffic Inspection

Traffic inspection is performed by an information system positioned between a client mobile device and external resources (e.g., the internet). This information system is typically implemented as a proxy server, application gateway, or portal, or through network flow auditing or packet inspection.[24] The proxy server accepts requests from the client mobile device for resource access, analyzes and processes the requests, forwards them to the appropriate resources, and returns responses from the resources to the client mobile device.

Network flow auditing or packet inspection is done through a network tap, or by configuring a network switch port into monitoring/copying mode to forward all packets to a collection device. The device may generate network flow records or other types of aggregated data as well as provide raw packet storage and warehousing. Analysis probes can also be installed close to the service network's edge within the service provider network or directly on a server, such as an SMTP or application server, to ensure true end-to-end network auditing. It is essential that the traffic inspection infrastructure have its clocks synchronized using NTP.[25]

Many characteristics associated with traffic inspection in a wired LAN, wireless LAN, and telework infrastructure apply to a mobile infrastructure. Traffic inspection should not be limited to IP protocols, as illustrated by the example of an application gateway for MMS/SMS traffic that interfaces directly to the mobile network operator's infrastructure.

The following NIST SP 800-53 Revision 4 security control families support this security function: System and Communications Protection (SC) and System and Information Integrity (SI).

### 4.6.2 Packet Filtering

Network devices, such as a firewall or an application gateway, perform packet filtering.[26] These network devices perform traffic inspection for all communications data at the boundary between the protected network and the internet (or other network segment) and block traffic that is inappropriate. There are three basic types of packet filtering technologies:[27]

- *Stateless:* This inspection may be "lightweight," analyzing only the headers of the packets with no "state" kept to relate a packet to a specific information flow;
- *Stateful:* This inspection is similar to stateless packet filtering, but a state is kept between related packets; and

[24] NIST Special Publication 800-46, Guide to Enterprise Telework and Remote Access Security.
[25] Cisco, Network Time Protocol: Best Practices White Paper, document ID: 19643, http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml.
[26] NIST Special Publication 800-53, Recommended Controls for Federal Systems and Organizations, AC-4, SC-5.
[27] NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy.

- *Application:* This inspection is where not only the payload of each packet is analyzed, but also the information among related packets within a specific application (such as an email message) for validity according to some defined policy.

These packet-filtering technologies are not limited to network devices. Most major operating systems (e.g., MS Windows, Apple OS X, and Unix variants) incorporate some form of packet-filtering technology, but the adoption of these technologies in mobile devices is lagging.

Mobile-infrastructure-specific design characteristics for packet filtering include the following:

- The mobile infrastructure ingress from the internet is separated and segmented from the protected service network, and traffic is restricted between the two networks; and
- An architecture of stateful and application packet filtering technologies should be considered between multi-tiered backend networks.[28]

The following NIST SP 800-53 Revision 4 security control families support this security function: System and Communications Protection (SC).

### 4.6.3 Content Filtering

Content filtering is the process of monitoring network communications at the application layer, analyzing traffic for sensitive, inappropriate, and/or suspicious content. Agencies must perform content filtering on all traffic entering or leaving the mobile infrastructure segment of their network to restrict the types of information that may be transferred between mobile clients and the enterprise. For instance, if a virtual desktop environment is not in use, an agency may restrict personally identifiable information (PII) from being transmitted to mobile client devices.

The following NIST SP 800-53 Revision 4 security control families support this security function: System and Communications Protection (SC).

### 4.6.4 Logging

Logging is the generation, transmission, storage, analysis, and disposal of log diagnostic data. The logging security function includes a policy and infrastructure for the management of logs (including event, audit, error, configuration, installation, and debugging information) from operating systems, services, applications, and network devices. Logging also provides a foundation for capacity planning and a critical source of data for SIEM infrastructures. Additionally, logging helps to support the monitoring and audit, traffic inspection, and content filtering security functions.

- Logging captures diagnostic events that can be derived into security-relevant events through correlation with other discrete types of events, then directed to a log collection infrastructure

[28] NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.

(which can be either centralized or distributed) in near real time, where the events can be warehoused for further analysis. For example, logging may include metadata within network-access gateway logs such as:
  - session start date and time;
  - session authentication/authorization characteristics;
  - source/destination IP addresses, port numbers, byte counts, or packet counts;
  - protocol attributes;
  - user data capture (for some duration).
- Legal and privacy issues restrict the capture of personal data. Agencies adhere to policies and Federal laws regarding the captured log data.
- SIEM infrastructures and products greatly enhance the collection, orchestration, and analysis of mobile device logging data. Some systems collect a wide array of events in the network, system, application, and security domains. These systems provide a valuable tool for root cause analysis and reporting. The SIEM system should also integrate tightly with the mobile device infrastructure, including the MDM.

## 4.7 Reporting

An agency typically applies similar, if not identical, reporting requirements to a mobile infrastructure that already apply to the existing TIC infrastructure, including mandatory reporting to US-CERT. As such, there is no capability definition specific to the reporting security function. D/As should ensure that their reporting requirements include the reporting of lost mobile devices.

The following NIST SP 800-53 Revision 4 security control family supports this security function: Incident Response (IR) and Communications Protection (SC).

## 4.8 Incident Response

The response security function encompasses all facets of incident response. Effective incident response requires effective processes and procedures for the six phases of incident response: preparation, identification, containment, eradication, recovery, and follow-up. The response security function is supported by traffic inspection (INS) and content filtering (CF) security functions and directly informs the reporting (REP) security function.

The following NIST SP 800-53 Revision 4 security control family supports this security function: Incident Response (IR).

# Appendix A Mobile Security Capabilities by Security Function

The capabilities listed in Table 13 outline the technical recommendations and guidelines to properly design, secure, manage, and operate a mobile infrastructure. Each capability is mapped to a set of NIST SP800-53 Rev 4 controls that, when used in combination, implement the capability. The capabilities in Table 13 are sorted by security function. NIST SP 800-53 Rev 4 security control identifiers and family names are provided in Table 12 so that a more detailed mapping of the capabilities can be made.

*Table 12: NIST SP 800-53 Rev 4 Security Control Identifiers and Families*

| ID | Family | ID | Family |
|---|---|---|---|
| **AC** | Access Control | MP | Media Protection |
| **AT** | Awareness & Training | PE | Physical & Environmental Protection |
| **AU** | Audit & Accountability | PL | Planning |
| **CA** | Security Assessment & Authorization | PS | Personnel Security |
| **CM** | Configuration Management | RA | Risk Assessment |
| **CP** | Contingency Planning | SA | System & Services Acquisition |
| **IA** | Identification & Authentication | SC | System & Communications Protection |
| **IR** | Incident Response | SI | System & Information Integrity |
| **MA** | Maintenance | PM | Program Management |

The NIST SP 800-53 Revision 4 Security Control Family ID control numbers were added to Table 13. The control ID numbers are shown in the order that best matches the order of the verbiage that describes the capability (not alphabetical).

*Table 13: Capability by Security Function*

| Index | MSRA Section Reference | Capability Definition | NIST 800-53 Security Control ID |
|---|---|---|---|
| **1** | 3.1.2, 3.1.4, 4.1, 4.2 | The agency has documented and implemented comprehensive security policies for the mobile infrastructure based on current best practices for mobile device configuration. Policies include, but are not limited to<br>• Role-based access levels for mobile users<br>• Authorized use of mobile devices | AC-1<br>AC-19<br>PL-1<br>PS-6<br>SA-2 |
| **2** | 4.1, 0, 3.1.5, 3.1.6 | A mobile infrastructure risk assessment is performed to understand mobile infrastructure threats, the likelihood that those threats will be realized, and the potential impact of realized threats on the value of the organization's assets. | CA-1<br>CA-2<br>RA-3 |
| **3** | 4.4.3 | The agency has documented and implemented a comprehensive mobile app assessment and validation capability that complements and supports its enterprise assurance and validation requirements. | RA-5<br>SA-2<br>SI-2<br>PM-9 |
| **4** | 4.1 | For all risks identified in the Mobile Security Reference Architecture, an agency performs the following tasks, as identified in the NIST publication 800-39 Appendix E:<br>• Risk framing<br>• Risk assessment<br>• Risk response<br>• Risk monitoring | PM-9<br>RA-3 |
| **5** | 3.1.1,<br>4.1, 4.5 | All devices in the mobile infrastructure with cryptographic functions must be FIPS validated. Refer to http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm for a list of all vendors with a validated FIPS 140-2 cryptographic module. | SC-12<br>PL-1<br>PM-1<br>SA-1<br>SC-13 |

| | | | |
|---|---|---|---|
| **6** | 3.1, 4.1, 4.6 | Requirements for a mobile infrastructure Network Intrusion Detection System (NIDS) are based on:<br>• Technical, operational, and business goals/objectives of current system/network environment (e.g., network diagrams, OS, applications) and the mobile system<br>• Existing security protections (e.g., existing IDPS implementations, centralized logging)<br>• Types of threats for which the NIDS provides protection<br>• Monitoring requirements on network use and violations of acceptable use | PM-1<br>PM-11<br>PM-15<br>SA-8 |
| **7** | 3.1, 4.1, 4.2.2 | Agency security personnel with required skill sets are employed during design, implementation, and operation of the mobile infrastructure. If an agency's personnel do not have the requisite skill sets, the services of security professionals who have the required skill sets are employed to assist during design, implementation, and operation of the mobile infrastructure. Agencies ensure allocation of adequate funding to operate, maintain, and modernize the mobile infrastructure to meet emerging threats. | PM-3<br>PM-13<br>PS-1<br>PS-2<br>PS-3<br>PS-4<br>PS-5<br>PS-6<br>SA-2<br>SA-3<br>SA-8 |
| **8** | 4.1, 4.1.2 | A fallback strategy has been established in case of mobile authentication failure. For example, a fallback strategy to provide access to an authorized user in case of a forgotten password and/or lost smart card. A fallback strategy can be a technical process or may involve a human process that is at least as strong as the primary authentication method. | IA-1<br>IA-2<br>IA-3<br>IA-6<br>PL-2 |
| **9** | 3.1.2, 4.1, 4.4 | Agency management establishes a mobile infrastructure configuration baseline and Change Control Board (CCB) to formally track modifications and maintain a proper baseline. | CM-1<br>CM-2<br>CM-3<br>CM-4 |
| **10** | 4.1, 0 | Only agency-authorized mobile devices and associated staff are allowed to access the mobile infrastructure with predefined roles. | AC-1<br>AC-2<br>AC-3<br>AC-6<br>AC-19<br>IA-8 |

| | | | |
|---|---|---|---|
| **11** | 4.1, 4.6 | The agency designates an individual or group to track mobile infrastructure product vulnerabilities and wireless security trends. | PL-1<br>PM-12<br>PM-15<br>SI-4 |
| **12** | 4.1.1 | Mobile security training is part of the agency's overall security training program and is mandated regularly (e.g., annually). Mobile infrastructure administrators receive proper training as mobile technologies evolve.<br>Users are educated about the risks of mobile technology and how to mitigate those risks. Mobile security training includes mobile security awareness, policy overview, and the following guidelines:<br>1) Maintain physical control over mobile devices.<br>2) Protect sensitive data on mobile devices with FIPS-approved encryption (e.g., data stored is encrypted).<br>3) Disable wireless interfaces on mobile devices when not needed. (This guideline is separate from voice services on the mobile devices.)<br>4) Report lost or stolen mobile devices promptly. | AR-5<br>AT-1<br>AT-2<br>AT-3<br>AT-4<br>PL-4<br>PM-14<br>PM-16 |

| | | | |
|---|---|---|---|
| **13** | 4.1.2 | A physical security plan is provided to ensure that mobile infrastructure components are securely installed to prevent unauthorized tampering, and can only be accessed by authorized personnel.<br>All operations and management of the physical infrastructure that supports the mobile device service infrastructure is covered by the plan. | PE-1<br>PE-2<br>PE-3<br>PE-4<br>PE-5<br>PE-6<br>PE-8<br>PE-9<br>PE-10<br>PE-11<br>PE-12<br>PE-13<br>PE-14<br>PE-15<br>PE-16<br>PE-17<br>PE-18<br>PL-2 |
| **14** | 3.1.2, 3.1.4, 4.2 | Two-factor authentication is required for agency-credentialed users who access the mobile infrastructure remotely. | AC-3<br>AC-19<br>IA-1<br>IA-2<br>SC-8 |
| **15** | 3.1.2, 3.1.4, 4.5 | Two-factor authentication is recommended for agency mobile infrastructure administrators accessing the mobile infrastructure from the local network.<br>Restrict authenticators to specific roles and actions. | AC-3<br>AC-19<br>CA-3<br>IA-1<br>IA-2<br>IA-5<br>IA-6 |

| | | | |
|---|---|---|---|
| **16** | 4.3.1, 4.5 | Authorized mobile client users encrypt files stored on mobile devices and removable media. Encryption is accomplished by the use of FIPS 140-2 compliant whole disk or file encryption software. | DI-1<br>DM-1<br>IA-7<br>MP-1<br>MP-2<br>MP-3<br>MP-4<br>MP-5<br>MP-6<br>MP-7<br>SC-12<br>SC-13<br>SC-17<br>SC-28 |
| **17** | 3.1, 4.1, 4.3.2, 4.6.4 | Security audit processes and procedures are in place to identify the types of security-relevant events that are captured and stored. Audit records are securely stored for subsequent analysis. | AU-1<br>AU-2<br>AU-3<br>AU-4<br>AU-9<br>PL-1<br>PL-2 |
| **18** | 3.1, 4.4 | Operating system and application security configuration standards exist for:<br>• Mobile client devices to account for mobile security risks<br>• Virtual desktop environment<br>• Sandboxed environments<br>• Wireless access<br>• VoIP | AC-18<br>AC-19<br>CA-9<br>CA-2<br>CM-6<br>CM-7<br>CM-9<br>CM-10<br>CM-11<br>SC-15<br>SC-18<br>SC-19<br>SI-10<br>SI-16 |
| **19** | 4.1 | Agency-authorized mobile client devices have appropriate host-based defenses. | PM-12<br>SC-7<br>SI-4 |

| | | | |
|---|---|---|---|
| **20** | 3.1.2,<br>0, 4.1, 4.4.2 | Mobile infrastructure software patches and upgrades are tested and deployed regularly; the system baseline is updated as approved by the CCB. | AC-19<br>CM-1<br>CM-2<br>CM-3<br>CM-9<br>MA-1<br>MA-2<br>MA-6<br>PL-1<br>SA-11<br>SI-2<br>SI-7 |
| **21** | 3.1, 4.1, 4.2.2 | An inventory is maintained of all mobile infrastructure equipment, including but not limited to:<br>• Authorized mobile client devices<br>• VPN concentrators<br>• Virtual desktop environments<br>• NIDS equipment<br>• Firewalls<br>The inventory information includes, but is not limited to:<br>• MAC addresses<br>• Device model numbers<br>• Device serial numbers<br>The acquisition process for all mobile devices (and all supporting infrastructure) is procured through approved vendors. | CM-8<br>PL-1<br>PL-2<br>PM-1<br>PM-5<br>SA-4 |
| **22** | 3.1.2, 4.1, 4.3, 4.6 | When disposing of mobile infrastructure components, ensure that:<br>• All sensitive configuration information is removed, including data stored on the devices and passwords.<br>• The component's audit records are retained as needed to meet legal or other requirements.<br>Simple deletion of configuration items might not result in complete destruction of the information because the deletion process is vendor- and implementation-specific. | AC-22<br>AU-1<br>AU-9<br>DM-2<br>CM-9<br>MP-6<br>PL-1<br>PL-2<br>SC-28 |

| | | | |
|---|---|---|---|
| **23** | 3.1.2, 4.1 | The agency's security configuration standard is re-applied whenever a mobile infrastructure device is reset, replaced, or rebuilt. | CM-6<br>CM-9<br>PL-1<br>PL-2 |
| **24** | 3.1.5,3.1.9,4.6.1 | The NIDS is able to import traffic captures from external sources, such as commercial capture software, tcpdump, or network traffic analyzer. NIDS can replay the captures through the NIDS detection engine. | SC-7 |
| **25** | 3.1.2,4.6 | The NIDS allows administrators to selectively activate and deactivate the display of individual/unique alarms and events. | AC-8<br>AC-17<br>CA-7<br>SC-7 |
| **26** | 4.6 | The NIDS supports the following:<br>• Standardized logging and report formats<br>• Export of event logs to industry standardized formats<br>• Association of log entries to corresponding external references, including Common Vulnerabilities and Exposures (CVE) numbers and vendor security advisories. | CA-7<br>SC-7 |
| **27** | 3.1.6,3.1.9,4.6 | The NIDS is deployed to detect suspicious or unauthorized activity. Device monitoring includes recording IP addresses of unauthorized clients. | CA-7<br>SC-7 |
| **28** | 3.1.6,3.1.9 | The NIDS is configured with custom signatures to meet agency needs, including the application-layer signatures and critical signatures published by US-CERT, and their agency CERT, as applicable. | SC-7 |
| **29** | 3.1.6,3.1.9,4.6 | In addition to sample events described in the *Logging* section, the NIDS detects and logs attack signatures (including user-defined signatures), performs stateful frame inspections, and captures attacks spanning multiple frames. | CA-7<br>SC-7 |
| **30** | 3.1 | The mobile infrastructure LAN is separated and segmented from the main agency LAN, and traffic is restricted between them. The defined filtering policy should be based on agency risk assessments, and user requirements for access to agency network resources. | PM-9<br>SC-7 |

| | | | |
|---|---|---|---|
| **31** | 4.3.1 | The agency has a data loss prevention program applicable to its mobile infrastructure, and follows a documented process for data loss prevention. | DI-1<br>SC-7 |
| **32** | 4.6.4 | At a minimum, the NIDS logs event information, such as timestamp, event type, source of the event, the sensor or agent that detected the event, and supporting data involving the details of the event. (The sensor can monitor Wi-Fi and may not be able to monitor voice and 3G activities.) | AU-2<br>CA-7<br>SC-7 |
| **33** | 4.6.4 | Logging is activated to capture mobile infrastructure-specific events, and log entries are directed to a central monitoring and auditing server for review and audit. | AC-21<br>AC-22<br>CA-7<br>SC-7<br>SI-4 |
| **34** | 4.3.2,4.6,4.7 | Audit logs are reviewed on an agency-defined time interval based on risk assessment and Federal guidance.<br>Audit logs can also profile the use of the mobile service infrastructure by both the management team and end users. | AU-1<br>AU-2<br>AU-3<br>AU-6<br>AU-7<br>AU-8<br>AU-11<br>AU-12<br>AU-13<br>CA-7<br>SC-7<br>SI-4 |
| **35** | 4.1, 4.2, 4.7, 4.8 | At a minimum, the agency annually conducts and documents a security review of the mobile infrastructure and undertakes the necessary actions to mitigate risk to an acceptable level based on the mobile infrastructure's FIPS category. Vulnerability scanning of the mobile infrastructure is a component of the security review. | PM-9<br>RA-1<br>RA-3<br>RA-5 |
| **36** | 3.1, 4.2.3 | The mobile infrastructure design includes the capability to terminate or quarantine mobile operations in the event of an emergency. | AC-19<br>SA-8 |

| | | | |
|---|---|---|---|
| **37** | 4.1, 4.8 | The agency has a documented and operational incident response plan in place that defines actions to be taken during a declared incident. In the event of a declared incident or notification from US-CERT, or their agency CERT, as applicable, agency operations personnel immediately activate incident response plans. | IR-1<br>IR-3<br>IR-4<br>IR-5<br>IR-6<br>IR-7<br>IR-8<br>IR-9<br>PL-1<br>PL-2<br>SE-2 |

# Appendix B Mitigating Common Mobile Device Threats

Mobile devices[29] face some of the same threats as desktop computers. However, these devices are subject to many additional unique threats because of their size, portability,[30] services, and unique architectural features. Depending on which services are implemented or activated, these additional threats can increase the device's vulnerability to interception, alteration, and injection of traffic. This appendix summarizes of mobile device security threats as well as key security guidelines for mitigating mobile device security threats when these devices are used to access D/A enterprise assets. Each D/A may customize the guidelines based on its business and operational deployment requirements by taking into account the associated risks and security implications.

## B.1 Software-Based Threats and Mitigations

Mobile devices provide many of their benefits and capabilities to a user through native software or through applications and system software enhancements that a user can download and install. Smartphones and tablet computers have become popular because of their ease in selecting and installing these applications and system enhancements. Unfortunately, some of the applications and enhancements can be malicious in their intent.

### B.1.1 Malware Threats

Malware, or malicious code, is software written with the intent to perform an unauthorized action that will compromise the confidentiality, integrity, or availability of the mobile device. Malware can be attached to instant messages, appended to electronic mail, or downloaded as an infected file via the internet.[31] Malware may also be embedded in downloaded applications. Malware can affect the operation of the mobile device operating system, compromise data or applications on the mobile device, or both.

#### Malware Mitigation

- The security of a mobile system depends on the security of a chain of components that include the hardware, operating system (OS), application repository, application development principles, and the D/A's operational and managerial control of such systems. D/As should choose the hardware platform that is most resistant to vulnerabilities; D/As should also select an OS and specific versions of that OS that are resistant to most vulnerabilities. Actor(s): mobile device operating system developer, mobile device manufacturer, government agency.

[29] Threats for mobile devices derived from Bohne, Crossler, Field, Keppler, Carlson, McNab, Sheriff, and Sweitzer (The MITRE Corporation). "A Security-Driven Approach to Developing Mobile Solutions." September 8, 2011.

[30] Jansen, W. and Scarfone, K. (NIST). *NIST 800-124: Guidelines on Cell Phone and PDA Security,* Pg. 3-1, October 2008. http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf.

[31] Jansen, W. and Scarfone, K. (NIST). *NIST 800-124: Guidelines on Cell Phone and PDA Security,* Pg. 3-2, October 2008. http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf.

- D/As should develop policies and procedures regarding the use, purchase, and installation of applications. D/As should evaluate the use of access policies that use a whitelist approach to application installation. Actor(s): government agency, mobile device manager.
- D/As should provide user awareness training and impose security policies explicitly stating that users are forbidden to install unauthorized applications. In addition, D/As should implement application detection features on mobile devices. Actor(s): government agency, mobile device manager, mobile device consumer.
- Firewalls and signature-based malware scanners can detect malware in real time and take steps to block or isolate the threat. However, considerations such as limited battery life and connection bandwidth, may make these options power- and cost-prohibitive. Some mobile devices do not have a user configurable local firewall. Actor(s): government agency.
- If available, basic firewall settings should be applied to mobile devices, and pre-scheduled virus scanning should be performed with minimal user impacts (e.g., after hours with direct power charging on weekly basis). Additionally, D/A-internal network firewalls, in concert with other security services, such as proxies and content filtering, should be used to protect mobile devices when they are connected to internal networks. Actor(s): government agency.
- The use of environment virtualization (i.e., “sandboxes”) can enhance security by restricting access of applications to the OS (or limiting access of the OS to applications, depending on whether the sandbox is an agency sandbox in a non-GFE device or a personal-use sandbox in a GFE device). System monitoring, wiping, and other functions can be carried out at the sandbox level. Actor(s): government agency, mobile device manager.
- D/As should use a centralized application to manage mobile devices; to enable enterprise-wide configuration management of essential features, such as over-the-air policy pushes and enforcement; remote wiping; and application use restrictions. Some MDM products do not support all features, so the administrator must verify that the D/A’s desired set of OS policies can be implemented by the chosen MDM product. Actor(s): government agency, mobile device manager.

## B.2 Exploitation of Vulnerable Mobile OS

Vulnerabilities in mobile operating systems and applications, similar to those for desktop computers, are discovered constantly. Operating system vulnerabilities can be exploited in a manner similar to vulnerable applications. Operating system vulnerabilities can pose a greater threat because the operating system runs at a higher privilege level than applications. Mobile applications, like applications on other devices, can also be poorly written and vulnerable to attack and exploit. Many applications are vulnerable due to programming errors, design flaws, or configuration choices in security relevant capabilities.

A “hacker” culture has arisen around devices in which groups of users disable the native OS security features, commonly known as “jailbreaking” or “rooting.” Disabling the native OS security features allows users to install applications and system enhancements that would otherwise be restricted. For example users could then download apps without the use of official online application stores. In general, the process used to bypass native security features is published within hours or days of new OS releases. There is a high-level risk associated with the use of altered devices, and manufacturers have taken many steps to prevent this alteration, but the pervasive nature of reverse engineering and the publication of key system characteristics has enabled hackers to continue to bypass native security functions.

#### Exploitation of Vulnerable Mobile OS Mitigation

- D/As should ensure that mobile devices comply with D/A-specified security configuration settings and have the latest software patches installed. Non-compliant devices can have access to enterprise assets suspended until all required patches are installed. Actor(s): mobile device manager, mobile device app developer, mobile device operating system developer.
- D/As must constantly evaluate the latest OS release and determine installation schedules with deadlines. Although a mobile device may arrive installed with the most current firmware when it was purchased, new updates, including bug fixes and security fixes, are being made available frequently. [32] D/As should include mobile devices in existing patching and remediation regimens, checking for software updates regularly. Actor(s): government agency, mobile device manager, mobile device operating system developer.
- D/As should also enable integrity checks on device operating systems to detect rooting and jailbreaking. Devices that are compromised should be disabled and examined. Actor(s): government agency, mobile device manager.

### B.2.1 Exploitation of Vulnerable Mobile Application

Vulnerabilities in mobile device applications represent a threat similar in nature to those presented by desktop or laptop computer applications. The culture associated with mobile devices makes it easy and attractive to install additional applications. Rooting or jailbreaking enables unauthorized programs or applications to be installed on mobile devices. These installations could introduce malware into devices, either intentionally or unintentionally, by bypassing D/A security policies and restrictions. Malware is found in applications from both vendors and markets, and from uninvited spam via text messages or emails. Additional vulnerabilities may be introduced by poorly written applications that reduce the security posture of a device.

#### Exploitation of Vulnerable Mobile Application Mitigation

- A D/A should use information security policies with continuous monitoring capabilities to track mobile device assets and their security postures to ensure that mobile assets comply with D/A-specified authorized application lists. Non-compliant devices can have access to enterprise assets suspended until all application installation issues are resolved. Actor(s): government agency, mobile device manager.

[32] NSA. “Security Tips for Personally Managed Apple iPhones and iPads,” Pg. 1, March 2011. http://www.nsa.gov/ia/_files/factsheets/iphonetips-image.pdf.

- When creating applications, programmers need to remove sensitive data properly. The operating system communicates a signal to all running applications that protected data is unavailable when the mobile device is locked. Programmers need to properly purge sensitive data from local memory and manage data-unreachable exceptions when the device locks. Actor(s): mobile device app developer.
- When developing secure applications for mobile devices, application programmers can perform the following actions to appropriately secure data in applications (assuming that users log into mobile devices via passwords):
  - Conduct a security assessment of the application architecture before the design is implemented by programmers; the security team should audit the architecture of the application and investigate issues, including whether is it necessary to store user credentials on the device. [33] Actor(s): mobile device app developer.
  - Validate the proposed application architecture against known flaws, such as those found in resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases.[34]
  - Require the use of official applications. Third party applications should be signed by a trusted entity, as allowed by the OS, to prevent unauthorized tampering or modification of application code. Actor(s): mobile device manufacturer, mobile device operating system developer, mobile device application developer.
  - Use the appropriate protection class for the data. Actor(s): mobile device app developer, mobile device operating system developer.
  - Use a key store to store sensitive identity information. The keychain can be used to store digital identities, user names, and passwords. It can be segmented so that one application cannot access another application's credentials.[35] Actor(s): mobile device operating system developer, mobile device consumer.
  - Developers need to use the appropriate protection class when storing sensitive data, such as credentials, inside a key store. Actor(s): mobile device app developer, mobile device operating system developer.

- One of the mechanisms that can limit the ability to install unapproved software or malware on devices is native or MDM provided functionality that requires applications to be installed only from a "whitelist" of approved applications. This limitation can be implemented with an agency-managed whitelist, or by limiting application access to those provided by an online application store (or an approved subset of store-provided applications). Actor(s): mobile device manager, government agency, mobile device app provider.

[33] Wang, Chenxi. (Forrester). "Building Secure iPhone and iPad Apps." June 7, 2011.

[34] NIST SP800-53 rev 4, Supplemental Guidance on Flaw Remediation (SI-2), May 7, 2013.

[35] Apple. "iPad in Business Security," Pg. 5, March 2011: http://www.directoraccess.com/pdfs/iPad_Security.pdf.

- When approving applications for use, or adding them to a “whitelist,” D/As should verify that the secure coding principles outlined above are incorporated into the mobile app, where possible. Mobile applications should be tested or vetted through a security testing tool prior to deployment, if such testing is supported by the development environment. Additional information and guidance is available in the Defense Information Systems Agency’s Mobile App Security Requirements Guide[36]. Actor(s): government agency.

## B.3 Web-Based Threats and Mitigations

As more devices access the Internet, web-based threats will continue to grow in size and sophistication, and will undoubtedly target tablets, smartphones, and specialized devices and services (e.g., Internet, television, and radio).

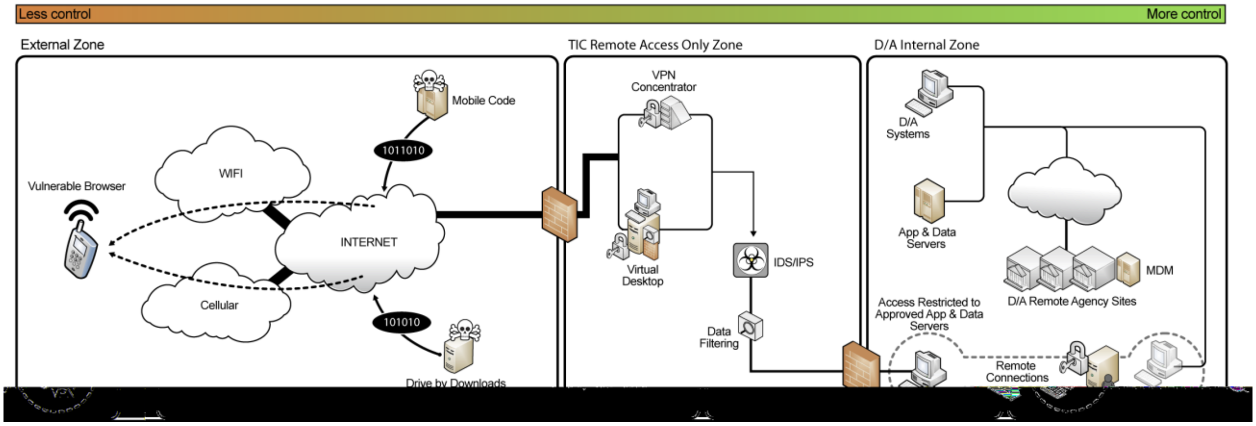

*Figure 13: Web-based Threats*

### B.3.1 Mobile Code

Mobile code is active content received via the network that can then be executed on the mobile device. Mobile code can be delivered through Hypertext Markup Language (HTML) 5, JavaScript, Adobe Flash, and other applications that support interpreted languages.

#### Mobile Code Mitigation

- To mitigate the threat of malicious mobile code accessed using web services, the D/A should employ the same protections for mitigating the threat from malware. In addition, the D/A can implement policies to disable active code processing by disabling JavaScript or limiting JavaScript access to official or authorized websites. Actor(s): government agency, mobile device manager.

### B.3.2 Drive-by Downloads

[36] Defense Information Systems Agency (DISA) Field Security Office (FSO) Security Requirements Guide (SRG) for Mobile Apps. http://iase.disa.mil/srgs/draft-srgs/.

The automatic delivery of malicious code as a result of a user visiting a website is a “drive-by download.” Drive-by downloads are extremely dangerous since the targeted individual does nothing to be at risk except visit an infected site, and many of the sites carrying the malware are legitimate sites that have been infected.

#### Drive-by Downloads Mitigation

- The threat posed by drive-by downloads can be mitigated using certificates, tokens, or other means of signature checks to minimize the possibility that a user connects to an untrusted service. In addition, using visualization virtualization and/or application gateways, such as web proxies, can enable the mobile device to use existing enterprise filtering for web traffic. Actor(s): mobile device application developer, mobile device application provider, government agency.

### B.3.3 Exploitation of Vulnerable Browser

A vulnerable browser is a special case of a vulnerable application for several reasons. First, a mobile device’s browser is an application that is used frequently, thus increasing the likelihood of threat exposure for the user. Second, there are many instances of malicious web content lying in wait on internet websites designed to take advantage of vulnerable browsers. Third, users may install and use non-default browsers that may not be managed or properly secured by the D/A, increasing the footprint of browser vulnerabilities.

#### Exploitation of Vulnerable Browser Mitigation

- To minimize the threats posed by a vulnerable browser, the D/A must be vigilant in tracking security assessments of browsers used by the D/A. The D/A should also implement security policies to ensure the latest verified and approved version of the browser is installed on all D/A mobile devices. Mobile access to official websites must require the use of a secure connection (e.g., D/A VPN service). Actor(s): mobile device application developer, mobile device application provider, government agency, mobile device manager.
- To ensure the D/A is using the strongest possible security settings for a web browser,[37] it must evaluate and determine the appropriate use for the following:
  - Turn off JavaScript. JavaScript is a client-side scripting language that enables developers to manipulate page elements, such as opening and closing windows or executing Java applets. JavaScript can be turned on before surfing trusted sites or when using the TIC security stack, but otherwise disabled in security-conscious settings.[38] Actor(s): government agency, mobile device manager.
  - Verify website certificates to prevent users from visiting a suspected phishing site that pretends to be a genuine site, such as a health-care provider. This approach helps to prevent

[37] Apple. “iOS: Safari Web Settings.” Updated October 12, 2011. http://support.apple.com/kb/HT1677.

[38] NSA. “Security Tips for Personally Managed Apple iPhones and iPads,” Pg. 2, March 2011. http://www.nsa.gov/ia/_files/factsheets/iphonetips-image.pdf.

suspect sites from capturing the user's sensitive information. Actor(s): mobile device application developer, mobile device application provider, mobile device manager.

- Turn off the browsing history to help prevent websites from monitoring users by not actively recording the pages visited, previous searches, or information entered into forms. Actor(s): mobile device application developer, mobile device application provider, mobile device manager.
- Enable "do not track" or "tracking protection" features of modern web browsers to request that websites do not track users' activities for purposes such as behavioral advertising.[39] If the mobile operating system supports such features, "do not track" should be enabled at the OS level. Actor(s): mobile device application developer, mobile device application provider, mobile device manager.
- Educate users about search-provider privacy policies and potential tracking if they are signed in when using search-provider services. Actor(s): mobile device consumer.
- Clear cookies between browser sessions or disable them entirely. Actor(s): mobile device application developer, mobile device application provider, mobile device manager.
- Hide or obfuscate information that identifies the browser as a mobile platform in exchanged messages (e.g., HTTP GET requests). Actor(s): mobile device application developer, mobile device application provider, mobile device manager.
- Prohibit mobile devices from direct data connections to the internet, and instead require them to use standard IT environment application gateways or visualization virtualization. A D/A can leverage their existing telework and Trusted Internet Connection infrastructure to provide a protected path to the internet. Actor(s): government agency, mobile device manager.
- Monitor and control the use of alternate, non-default browsers. Actor(s): mobile device manager.

## B.4 Network-Based Threats and Mitigations

Network-based security threats (Figure 14) are threats that have the potential for a threat-source to exploit vulnerabilities via the network at application layers or within applications, document files, or data (i.e., the data/service plane), as well as within the control plane, which is responsible for the configuration and management of the device. Network-based security threats initiate within the network and network protocols, as well as the devices, applications, and data that reside on the network. Mobile devices compound the problem of network-based security threats since they rely on Wi-Fi and cellular networks for communication. Devices that use Wi-Fi and cellular network communications are more accessible and exposed than hardwired devices.

[39] Mozilla. "Do Not Track." February 23, 2012. http://dnt.mozilla.org/.

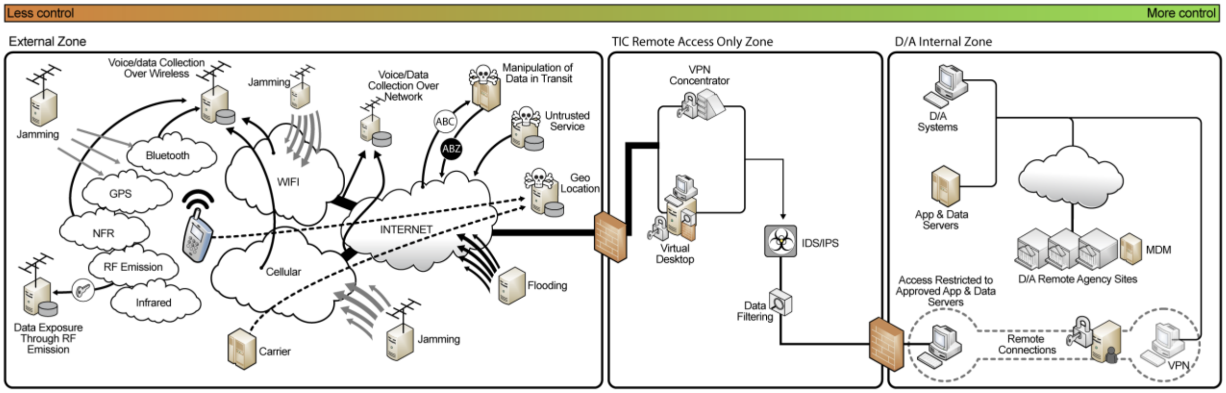

*Figure 14: Network-based Threats*

### B.4.1 Voice/Data Collection Over the Air

Mobile devices use several wireless protocols for communication that can be intercepted or compromised. Most devices support Wi-Fi, cellular, and Bluetooth wireless protocols.

**Wi-Fi**

Mobile devices use Wi-Fi wireless network communication based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g/n family of standards. These devices can connect to any mobile hotspot, personal or enterprise access points, or similar devices for peer-to-peer communication. Devices using Wi-Fi communications are vulnerable to interception by other Wi-Fi devices and wireless software tools, as well as by signal analyzers. Rogue access points (unauthorized imposters within an administratively managed domain) are also a potential threat, exposing the mobile devices to man-in-the-middle exploits.[40]

**Cellular (Mobile Carrier)**

Mobile devices can also communicate via cellular networks. Devices may be capable of supporting Global System for Mobile Communications (GSM), which AT&T provides, and Enhanced Data rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), High-Speed Downlink Packet Access (HSDPA) and High-Speed Uplink Packet Access (HSUPA), and Code Division Multiple Access (CDMA), which Verizon uses, Evolution-Data Optimized (EV-DO), and Long Term Evolution (LTE) protocols to receive and send data across cellular networks. Cellular Message Encryption Algorithm (CMEA) is a block cipher used for securing CDMA, and KASUMI (A5/3) encryption system is a block cipher used in UMTS, GSM, and GPRS, and EPS Encryption Algorithms (EEA) is based on SNOW3G and AES and is used for securing LTE mobile communications systems.

[40] NIST SP 800-48 R1, Guide to Securing Legacy IEEE 802.11 Wireless Networks, Chapter 5, Threats and Vulnerabilities.

Data and voice traversing over the mobile carriers' managed network can be intercepted and the configuration as well as core components can be compromised via control plane channels.

**Bluetooth**

Bluetooth is a low-power, short-range wireless technology that provides a standards-based wire-replacement protocol for connectivity. Bluetooth is used for both data transmission between devices within a personal area network (PAN) and for command as well as voice communications between a device and headset. Bluetooth provides native encryption and authentication mechanisms, but also has known vulnerabilities and exploits, such as a key negotiation hijack attack during session initialization.[41]

**Infrared Communication**

Infrared is a low-power, short-range wireless technology in the infrared spectrum that provides standards-based wire-replacement protocol for connectivity (RC-5, SIRC). Infrared is used both for data transmission between devices within a personal area network (PAN), and for command (one-way transmission). Infrared provides no encryption and authentication mechanisms, and thus has known vulnerabilities and exploits. Most vulnerabilities are vendor specific, such as the existence of a buffer overflow in the receiving infrared communications code.

**Near Field Communication**

Near field communication (NFC) is a set of standards for a low-power, ultra-short-range wire-replacement tool for point-to-point communications that is starting to be used for identification cards and credit and debit card transactions as of Q1 2012. NFC implementations are primarily subject to physical layer attacks, such as signal interception and injection, but specific implementations may contain additional vulnerabilities.

### Data/Voice Collection Over the Air Mitigation

- Minimizing the exposure of the mobile device to signal interception can mitigate the threat of data and voice collection over the air. The disabling of 3/4G network capabilities in high-threat areas such as foreign countries can accomplish this minimization. The mitigations for this threat include also disabling the Bluetooth, NFC, and 802.11 communications services,[42] if no secure VPN services or features exist on the device.[43] These VPN services and features should use strong network encryption and authentication techniques when accessing official network services. The security policy for mobile devices should also prohibit the dual-connection to multiple networks, known as "tethering" and "split-tunneling." Actor(s): mobile device

[41] NIST Special Publication 800-121, Guide to Bluetooth Security.

[42] Center for Internet Security. *Security Configuration Benchmark for iOS 4.3.3*.Version 1.3.0, Pg. 17, June 10, 2011. https://benchmarks.cisecurity.org/tools2/iphone/CIS_Apple_iOS_Benchmark_v1.3.0.pdf.

[43] Center for Internet Security. *Security Configuration Benchmark for iOS 4.3.3*.Version 1.3.0, Pg. 17, June 10, 2011. https://benchmarks.cisecurity.org/tools2/iphone/CIS_Apple_iOS_Benchmark_v1.3.0.pdf.

application developer, Mobile device application provider, Mobile device manager, Mobile device consumer.

- Federal enterprises should use the 802.1x protocol for connection authentication, which allows network-capable devices to be integrated with a broad range of authentication environments like Remote Authentication Dial In User Service (RADIUS).[44] This authentication is most often used in 802.11 wireless networking. Mobile devices may support one or more of the following 802.1x authentication protocols:[45] EAP-Transport Layer Security (TLS), EAP-Tunneled Transport Layer Security (TTLS), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Subscriber Identity Module (SIM), Protected Extensible Authentication Protocol (PEAP) v0/v1, and Lightweight Extensible Authentication Protocol (LEAP). Furthermore, a mobile device may be compatible with X.509 digital certificates[46,47] and recognize file extensions of .cer, .crt, and .der. The security policy on the mobile device should also prohibit simultaneous connections to multiple networks. Actor(s): mobile device application developer, mobile device application provider, mobile device manager, mobile device operating system developer.

### B.4.2 Voice/Data Collection Over the Network

Electronic eavesdropping can occur over the network. All communications will be routed over the wireless network (Wi-Fi or cellular) and through the internet to reach its endpoint.[48] Communications can be intercepted at the intermediary routing points or by various wiretaps and exploits.

#### Voice/Data Collection Over the Network Mitigation

- The risk level associated with the threat of data and voice collection over the network varies depending on the network being used for interception. For example, this type of threat has a low level of risk when the network is a D/A enterprise network. The level of risk is higher over a U.S. provider cellular network, and higher still if the network is in a foreign country. Security policies can be implemented to restrict data and voice network connections, but such a policy is not only impractical, it is difficult to implement a location-based policy. A practical mitigation strategy is to encrypt data in transit whenever possible. The encryption methods deployed must be FIPS validated to securely protect the data. Currently, there are an extremely limited number

[44] Australian Government Department of Defense. *iOS Hardening Configuration Guide: For iPod Touch, iPhone and iPad Running iOS 4.3.3 or Higher*, Pg. 27, June 2011. http://www.dsd.gov.au/publications/iOS_Hardening_Guide.pdf.

[45] Apple. "iPad in Business Security Overview," Pg. 2, April 2011: http://www.apple.com/ipad/business/it-center/security.html.

[46] Apple. "Deploying iPhone and iPad Security Overview," Pg. 4, October 2011. https://ssl.apple.com/ca/ipad/business/docs/iOS_Security_Mar12.pdf.

[47] Google, "Android Security Overview". March 2012, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_der_cred_ferraiolo_h_fips_201-2.pdf.

[48] Jansen, W. and Scarfone, K. (NIST). *NIST 800-124: Guidelines on Cell Phone and PDA Security,* Pg. 3-6, October 2008. http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf.

of mobile devices that have been FIPS validated. If a mobile device is not FIPS validated, D/As must ensure that a FIPS 140-2 application sandbox or virtualization solutions is used on the mobile device; otherwise, they should not allow any processing of D/A-sensitive data. D/As should provide detailed instructions regarding which network situations are high risk and should be avoided. Incidentally, some agencies have developed a VoIP application solution for secure voice communication on smartphone devices. Actor(s): mobile device cellular wireless carrier, government agency, mobile device application developer, mobile device application provider, mobile device manager, mobile device consumer.

- While MMS/SMS is a highly functional service, it may be unreliable (based on the carrier's QoS and SLA) and inherently insecure since data can be both observed and manipulated because intermediate transmission nodes (some being operated by third-party providers) are able to observe and copy messages. D/As that need SMS functionality should consider other methods of messaging that are encrypted and preferably IP based, and are based on open standards.[49] If an IP-based solution is not an option, third-party solutions for MMS/SMS encryption exist, and some may be FIPS 140-2 compliant. If a FIPS validated solution is unavailable, a risk assessment must be performed by the D/A and the risk approved by the appropriate Designated Approving Authority. Actor(s): mobile device application developer, mobile device application provider, mobile device manager, government agency, mobile device cellular wireless carrier.
- Training based on an active policy that informs users of the risks associated with using mobile devices in different network situations is also advisable. D/As should provide detailed instructions on which network situations are high risk and should be avoided. Actor(s): mobile device consumer, government agency.

### B.4.3 Manipulation of Data in Transit

Data and voice can be modified, manipulated, or selectively blocked while in transit to compromise the communication. One of the distinguishing attributes about mobile devices is that they frequently travel between communications mechanisms, whether hopping from one cellular tower to the next or transitioning from cellular to 802.11, and have limited computational and storage capacities when compared to their desktop and server companions. These attributes have led many mobile applications to rely on remote data stores, or data repositories that are not hosted on the mobile device, and offloaded processing for functionality. Hence, mobile computing has increased the amount of data in transit, which is traversing untrusted communication mechanisms. In addition, cloud services from device manufacturers and third parties offer users file storage, application data services, and management functions in a distributed environment, which mitigates limited on-device storage while increasing data exchanges between the cloud and the mobile device. The increase in data exchanges presents a larger attack space for an adversary to target D/A data in transit. This potential for sensitive

[49] P. Saint-Andre, Ed., IETF Network Working Group RFC 3920: *Extensible Messaging and Presence Protocol (XMPP): Core, October 2004,* http://www.ietf.org/rfc/rfc3920.txt.

information to be inadvertently disclosed due to a poorly implemented cloud architecture, a faulty implementation, or malicious activity, may make data storage or access by cloud-based applications a liability for Federal users.

### Manipulation of Data in Transit Mitigation

- Application-based encryption should be deployed to protect unencrypted application, service, and management data on mobile devices in transmission. Even though the application data may be encrypted, having an encrypted communication channel, reduces the risk of a covert entity observing the details of what applications are being used, or of service infrastructure behavior. The encryption methods deployed must be FIPS validated to avoid compromising sensitive data. Currently, not all mobile device cryptographic modules have been FIPS validated.[50] If a mobile device is not FIPS validated, D/As should not allow any processing of D/A-sensitive data without enhanced security controls. Actor(s): mobile device application developer, mobile device application provider, mobile device manager, government agency.
- To protect data in transmission, D/As should use the existing network remote access capability to allow mobile device users to securely access enterprise networks and resources via a VPN connection (e.g., SMS, NFC, Bluetooth, and other non-IP protocols should be encrypted as well, but are covered in other sections of this document). VPNs provide an end-to-end secure communication channel by enforcing strong authentication and encryption requirements and providing confidentiality and integrity protection for data in transit. For instance, two-factor authentication and public key infrastructure (PKI) certificates should be used for user and device authentication, and FIPS-140-2-compliant encryption methods for data encryption. VPNs should be activated when policy dictates; most mobile devices support VPN protocols, including Internet Protocol Security (IPSec), Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Secure Sockets Layer (SSL) VPNs[51] via applications available from various vendors. A user's VPN connection should be activated only when policy dictates and should include mandatory configuration settings such as timeout because malicious applications can exploit VPN services.[52] Actor(s): mobile device application developer, mobile device application provider, mobile device manager, government agency.
- If D/As have reservations (based on their security policies or on unknown levels of trust with a third-party service provider) about using cloud features, such as specific document sync, or backup, these features should be disabled through the mobile device's configuration profile or

[50] NIST FIPS 140-1 and 140-2 Vendor List, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

[51] Apple. "iPad in Business Security Overview," Pg. 3, April 2011. http://www.apple.com/ipad/business/it-center/security.html.

[52] Center for Internet Security. *Security Configuration Benchmark for iOS 4.3.3*.Version 1.3.0, Pg. 16, June 10, 2011. https://benchmarks.cisecurity.org/tools2/iphone/CIS_Apple_iOS_Benchmark_v1.3.0.pdf.

by using an MDM solution.[53] Actor(s): mobile device application developer, mobile device application provider, mobile device manager.

- File transfers can employ integrity verification mechanisms, such as hashes, to ensure that bulk data transfers are not modified en route. File fingerprinting techniques must not be easily spoofed, rarely collide, and produce mostly different hashes when small changes to the input file occur. File verification should be conducted on all executable code transferred to the mobile device. This verification can be accomplished through an MDM solution or manually through third-party hashing software. Actor(s): mobile device application developer, mobile device application provider, mobile device manager.
- When data is submitted by a mobile user to D/A infrastructure servers, an out-of-band confirmation mechanism can be employed. This confirmation can be in the form of a desktop accessible web page, call-back to the mobile user via voice, email confirmation with submitted data, etc. This confirmation increases security because the attacker must compromise both communications mechanisms to preserve stealth. Actor(s): mobile device application developer, mobile device application provider, mobile device manager, government agency.

### B.4.4 Data Exposure Through RF Emission

Most computational devices produce some radio frequency (RF) radiation due to the switching of discrete electrical components within the device itself, apart from integrated activated radios, such as cellular, Bluetooth, NFC, or Wi-Fi. This radiation is well within the RF spectrum and can be captured and decoded because the information radiated from the CPU and its subsystems is mostly unencrypted.

Almost all mobile devices that have this vulnerability are compliant with FCC part 15, which sets the controls for limiting the RF emission,[54] but which only protects the user from harmful radiation. As in any computing device, the vast majority of data manipulated by the CPU is unencrypted, and therefore vulnerable to observation by a third party, both in near proximity and from a distance (e.g., approximately 100 meters) using a high gain antenna, an RF receiver, an intermediate frequency amplifier, an A/D sampling converter, and a computational device. This configuration is very economical to produce and is becoming much smaller in size.

#### Data Exposure Through RF Emission Mitigation

- The private key capturing vulnerability is well known, and most vendors are beginning employ countermeasures, particularly in the smartcard domain. In the mobile device domain, vendors are limited to the following techniques address the problem:

[53] Apple. “Deploying iPhone and iPad Security Overview,” Pg. 4, October 2011. https://ssl.apple.com/ca/ipad/business/docs/iOS_Security_Mar12.pdf.

[54] Electronic Code of Federal Regulations (e-CFR), Title 47 Telecommunication, Part 15 Radio Frequency Devices, March 22, 2012, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title47/47cfr15_main_02.tpl.

  - *Obfuscation* breaks up the algorithm into multiple chunks of different lengths with slight delays between modules to remove the “double bump” signature of the exposed private keys. Actor(s): mobile device application developer, mobile device application provider
  - *Leak detection* uses shielding around the device that limits general RF from the CPU and other internal subsystems, but accommodates external antennas for normal wireless. telecommunication (e.g., cellular, Bluetooth, Wi-Fi). Actor(s): mobile device manufacturer, government agency, mobile device consumer.
  - *Balance* uses both hardware and software approaches. Actor(s): mobile device application developer, mobile device application provider, mobile device manager, government agency
- While D/As are limited to the vendors’ solutions to this problem, if they develop a mobile device application that uses RSA algorithms, they should at least use the software obfuscation technique to reduce the chance that the private key can be observed. Actor(s): mobile device application developer, mobile device application provider, mobile device manager.

### B.4.5 Connection to Untrusted Service

Mobile device users attempting to connect to a legitimate service can be fooled by a threat actor hosting an untrusted service; this deception can include legitimate service providers controlled by untrusted entities. The device can connect to an illegitimate service, allowing sensitive information to be exploited or compromised, posing a risk to the data’s integrity or confidentiality.

#### Connection to Untrusted Service Mitigation

- The threat posed by connecting to an untrusted service can be mitigated through user training about the risks posed by this threat and the steps a user can take to minimize the risks. The D/A should use strong encryption and authentication methods for accessing D/A enterprise resources and train users to recognize when a connection has not been properly established using strong security settings. Actor(s): mobile device consumer, government agency.

### B.4.6 Jamming

Jamming is a threat that interferes with the reception or transmission of wireless communications. Any wireless protocol that is used on a mobile device is vulnerable to jamming, including GPS, cellular, Wi-Fi, and Bluetooth.

#### Jamming Mitigation

- It is difficult to mitigate the threat of signal jamming on a mobile device. Users should be trained in the threat from jamming so that they can report jamming attacks when detected. Jamming threats to Wi-Fi networks in the D/A enterprise can be mitigated through the use of wireless intrusion detection systems or intrusion prevention systems (IDS/IPS), which detect the jamming and alert network administrators. Network administrators can then take steps to stop the jamming. Conversely, Bluetooth jamming is difficult to detect, diagnose, and mitigate without a considerable amount of effort, which may be economically unfeasible for the D/A. Actor(s): mobile device consumer, government agency.

### B.4.7 Flooding

A flooding attack inundates a system with more information than it can process. Any wireless protocol that is included on a mobile device is vulnerable to flooding, including GPS, cellular, Wi-Fi, and Bluetooth.

#### Flooding Mitigation

- As with jamming attacks, it can be difficult to stop flooding attacks on a mobile device. Malware scanners and the enforcement of D/A policies for acceptable applications can minimize the risk that malware on the mobile device is the cause of a flooding attack. Trusted facilities may have the capability to limit flooding (and jamming) by limiting signal penetration into the facility through rate reduction or filtering methods. It is essential that administrative domains constantly monitor for these flooding anomalies, in as close to real time as possible. Actor(s): mobile device application developer, mobile device application provider, mobile device manager, government agency.

### B.4.8 GPS/Geolocation

Almost all mobile devices provide some level of geolocation service capability in their applications. These applications may use this ability to display the current position on a map, locate nearby resources, or track the user's path. Even more popular with users is the ability of applications to provide driving directions. These location services have the potential to divulge the device's location (or provide inaccurate location information of the device user due to outside interference or manipulation).

**Geolocation Data Sources**

Collection of positional data from multiple data sources is a passive process, since all of the sources are broadcasting location information periodically with varying degrees of reliability based on the strength and noise level of the signal. Since the collection process is passive, there is no two-way authentication; therefore, the integrity of the positional data source could be suspect. Multiple positional data sources are used, which usually include:

- 2/3/4G mobile device signatures captured from cell nodes;
- Wi-Fi signatures (e.g., SSID, MAC address) mapped by a location service that has surveyed the Wi-Fi administrative physical domain area done via
  - an out-of-band third-party mapping service, such as the Google Maps survey cars
  - the carrier or a third-party application using the mobile device itself as a Wi-Fi signature sensor to send information back to the carrier or to a third-party mapping service
- Internal A-GPS receiver on the mobile device itself that passes the data to the carrier, OS/Application provider, or a third-party application provider.

**Triangulation**

By combining two or more positional data sources and through triangulation techniques, mobile device applications can greatly increase the accuracy and precision of their location while providing a dependable service when one or more of these sources become unavailable.

**Tracking**

Tracking via a mobile device's geolocation services is useful for many legitimate purposes, such as locating a lost device, but can also be used to gather intelligence or cause disruption for a D/A or individual. Illegitimate tracking can be performed by data mining and looking for geotagged records, pictures, or other data, or by examining and correlating use patterns.

**Geotagging**

Geotagging is the process of adding geographical identification metadata to various media such as photographs or videos. Data mining of geotagged pictures or other media recorded by the mobile device is a method that allows tracking for both legitimate and illegitimate reasons.

**Location Spoofing**

Covert GPS signals can be broadcast and false location information based on the locations of cellular towers, or Wi-Fi hotspots can be used to transmit erroneous location information. These attacks cause the mobile device to report an inaccurate location that would adversely affect applications that rely on accurate location data.

### GPS/Geolocation Mitigation

- Perform a risk tradeoff analysis to determine if GPS/geolocation capabilities are needed to run necessary applications or retrieve lost devices, or if the risk of tracking or spoofing is too great and the exposure of the tracking data maintained by the carriers is too high a risk. Unless these capabilities are deemed necessary, disable the device's tracking features through an MDM solution and audit the configuration regularly. When GPS/geolocation capabilities are required, minimize the use of third-party applications that use geolocation, which could lead to the tracking and storage of location data; deploy strong encryption methods for data on mobile devices to protect location information; and understand the risks posed by geolocation records kept by the mobile device, the provider network, or application providers. Actor(s): mobile device cellular wireless carrier, mobile device manager, government agency, mobile device application developer, mobile device application provider, mobile device operating system developer.

## B.5 Physical Threats and Mitigations

Not all security threats involve an adversary trying to corrupt or steal data. Some threats, such as misplacing a device, occur without any malevolent intent. Regardless, physical threats are becoming more and more common in the highly mobile workforce, as devices become smaller and more ubiquitous in nature.

### B.5.1 Loss of Device

The loss of a mobile device puts the confidentiality, integrity, and availability of the information on the device at risk. Further, the device could contain credentials to access enterprise resources, placing additional risk on the enterprise. Additionally, the data on the device may be lost if the device has not been backed up.

**Data Recovered by Unauthorized Party**

If the mobile device is lost or out of the physical possession of the device's legitimate user, then there is a chance that the data, configuration information, and credentials residing on the device could be recovered by an unauthorized party.

**Unauthorized Use of Authorized Credentials**

This threat shows that the identity of the device itself serves as a weak authenticator, since a lost or stolen device may provide access to the enterprise network. Cloning introduces an additional vulnerability since an attacker could configure another device to be an exact duplicate of a legitimate device, making it appear to be authentic to the enterprise network.[55] Finally, credentials can be stolen or misappropriated from the device, leaving the enterprise network vulnerable.

#### Loss of Device Mitigation

- To protect the confidentiality of data on a lost mobile device, a D/A should ensure the following:
  1. Strong passwords are required on all enterprise devices;
  2. A policy to wipe the sensitive data from the device is established;
  3. Technical controls are in place to allow for remote wiping either by administrator interaction, or through a device self-wiping after some preconfigured condition is met (e.g., amount of time without contact to infrastructure services [a.k.a. poison pill], repeated invalid authentication attempts); [56]
  4. Remote screen lock can be used to prevent unauthorized access to device contents until the device can be retrieved or wiped;
  5. A policy requires users to report lost and/or stolen devices within a prescribed amount of time to proper authorities;
  6. Geolocation services are remotely enabled, if available, to locate and retrieve the lost device;

[55] Jansen, W. and Scarfone, K. (NIST). *NIST 800-124: Guidelines on Cell Phone and PDA Security,* Pg. 3-7, October 2008. http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf.

[56] Apple. "iPad in Business Security Overview," Pg. 3, April 2011. http://www.apple.com/iphone/business/it-center/security.html.

7. A policy is established to require mobile devices be in the possession of the owners at all times unless properly secured (in accordance with protection guidelines for the sensitivity of the device and/or device contents);
8. Hardware and/or software encryption via FIPS 140-2 qualified techniques are provided to protect all data at rest on the mobile device; and
9. Users are prohibited from being able to disable data encryption.

Actor(s): mobile device operating system developer, mobile device application developer, mobile device application provider, government agency, mobile device manager, mobile device manufacturer, mobile device consumer.

- In most cases the strength of the data protection feature derives from the user's passcode because the user's passcode helps to generate the encryption key. When possible, the D/A should extend existing passcode policies to include mobile devices. In addition, consideration should be given to mobile-device-specific attributes, including the following:

1. limited user interface for character input;
2. possible need for rapid device accessibility;
3. number of failed attempts before wipe;
4. remote lock;
5. administrator reset passcode; and
6. whether the mobile device echoes or displays for a short period of time the characters typed into password fields.

Actor(s): mobile device manager, government agency, mobile device operating system developer, mobile device manufacturer.

### B.5.2 Physical Tamper

There is a potential for anyone who has physical access to a mobile device to install malicious hardware or software that could gather or corrupt data, either on the device or at the enterprise level, and introduce additional enterprise-wide security threats. An attacker could use external interfaces to attach the mobile device to a USB/Bluetooth tether. Additionally, an attacker may be able to connect a computer or external hard drive to clone, copy, destroy, erase, or modify device contents.

#### Physical Tamper Mitigation

- Some mobile devices have built-in tamper-proof features to minimize the risk of a threat actor tampering with a D/A device by purposely installing malicious software or hardware. Users should be trained on the importance of maintaining physical control of a device in high-risk situations (e.g., travel to a foreign country), and reporting suspicious instances when physical control was lost. Actor(s): mobile device manufacturer, mobile device consumer, government agency.

### B.5.3 Device-Specific Features

Built-in mobile device features, such as the camera and microphone, pose an increased security threat by creating a means to collect sensitive images or conversation. In some cases, third parties and criminals can turn on the microphone in your device even when you think it is turned off.[57]

#### Device-Specific Features Mitigation

- To minimize threats from device-specific features, only capabilities required for D/A work-related activities should be enabled. For instance, the built-in cameras and microphones should be disabled or blocked when not required. When cameras or other features are not required, preference should be given during product selection to models that do not contain these features. To prohibit cameras from being able to take pictures and video surreptitiously, a shield can be used, such as opaque tape or a case or cover that does not include a camera cutout. Additionally, the device features may be controlled based on predefined conditions being met, such as the camera being disabled only within certain regions. Actor(s): mobile device manufacturer, mobile device operating system developer, government agency, mobile device consumer.

### B.5.4 Supply Chain

The supply chain of the mobile device's components, assembly, and accessories provides an opportunity to physically tamper with the device before delivery and introduces exploits through the use of accessories.

#### Supply Chain Mitigation

- To minimize the threat of physical tampering of D/A assets prior to receipt, the D/A should only use trusted and verified supply sources, restrict the access of mobile devices not purchased from these trusted sources, and train users about information and communication technology (ICT) supply-chain threats, including counterfeit parts. GSA-qualified vendors and approved product lists can assist in identifying hardware and vendors that have been reviewed previously. Actor(s): mobile device manufacturer, mobile device broker, mobile device consumer, government agency.

### B.5.5 Mobile Peripherals

Products that physically interact with and/or augment the mobile device also pose potential risk. Docking stations, feature cases, and wireless peripherals can be used by an attacker to gain access to the mobile device.

[57] FBI. "Safety and Security for the Business Professional Traveling Abroad." February 23, 2012. http://www.fbi.gov/about-us/investigate/counterintelligence/business-brochure.

### Mobile Peripherals Mitigation

- In addition to the D/A providing a list of approved mobile computing platforms, it should consider providing a list of approved peripherals. User education programs should include instruction on appropriate use and security when connecting to peripherals. Actor(s): mobile device manufacturer, government agency, mobile device consumer.

## B.6 Mobile Device Threats to the Enterprise and Mitigations

The resources of the enterprise may be compromised if mobile devices are not secured and managed properly. These threats (Figure 15) can extend to user desktop and laptop computers, network servers, email, mobile devices, web servers, databases, and storage devices, and could allow an unauthorized user unrestricted enterprise access.

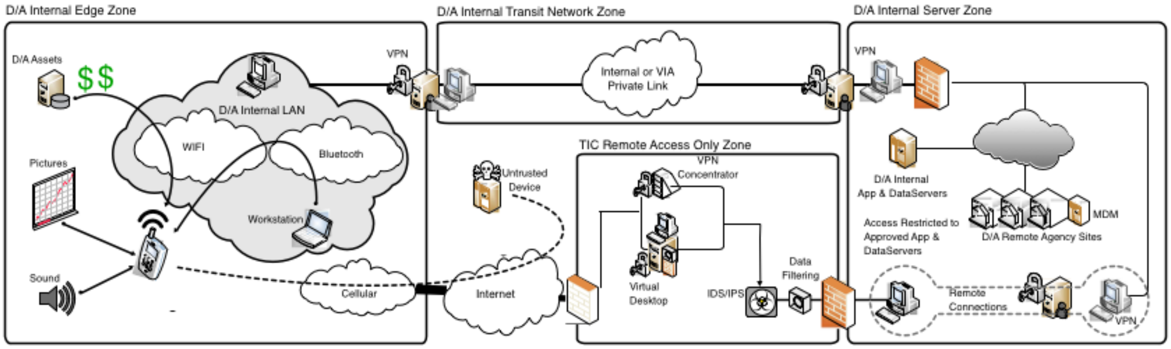

*Figure 15: Mobile Device Threats to the Enterprise*

### B.6.1 Access to Enterprise Resources

- A lost or stolen mobile device or compromised credentials may provide full access to sensitive information and resources within the D/A enterprise network. This access could result in enterprise data being compromised or malicious activities executed via mobile device access to enterprise data and the network. Also, sensitive information that is not digitized, such as hard copy documents, information from whiteboards, and conversations, can be digitized, captured, and transmitted easily from a covert individual's device. Because of its size, computational power, and array of input transducers (e.g., camera, microphone, accelerometer, GPS, Wi-Fi, Bluetooth), the mobile device is an important tool for espionage by covert organizations and threats from inside members of the D/A.

### Access to Enterprise Resources Mitigation

- The D/A should implement actions and systems to require authenticated proxy communication (with inspection if possible) to and from internal services (such as Exchange ActiveSync or BlackBerry Enterprise Server, Lotus Notes, etc.), require certificate-based authentication for email as well as Wi-Fi, deny access to internal resources not specifically allowed to mobile users (depending on D/A policy), deploy an auditing or security information and event management

(SIEM) solution, and document mobile device processes in incident response plans. Some D/As have developed their own technologies and strategies themselves to ensure that full access to enterprise data is limited. Actor(s): mobile device app developer, mobile device app provider, government agency.

- For D/A organizations with sensitive information in exposed areas, visitors should be asked to check their mobile device at the entrance of the D/A, and checked devices should be stored in a secure RF-shielded enclosure. Actor(s): government agency, mobile device consumer.

### Authentication Considerations

- To minimize the threat posed by a compromised or lost mobile device, agencies should leverage HSPD-12 compliant authentication solutions for Federal employees and contractors. For other users, the D/A should require authentication commensurate with the sensitivity level of the information at risk[58]. In most cases, this equates to using strong authentication tied to system authorization, authentication identity management, encryption (e.g., PKI, two-factor, etc.), and IDS/IPS methods for all enterprise resource access. These methods for remote access are identified in the telework reference architecture,[59] FIPS 140-2, and the TIC reference architecture.[60] Actor(s): mobile device app developer, mobile device app provider, mobile device manager, government agency, mobile device manufacturer.
- HSPD-12 Personal Identity Verification (PIV) Credentials are the government-wide standard for providing two factor authentication to Federal systems requiring “some” to “very high” level of identity assurance. NIST is currently finalizing FIPS 201-2 and developing a new special publication, 800-157 “Guidelines for Personal Identity Verification Derived Credentials” to provide guidance on how to leverage PIV credentials for use with certain mobile devices, such as tablets. For devices in which an HSPD-12 compliant solution is currently unavailable, agencies may leverage other alternate factors, as determined and sanctioned by Federal standards. For individuals for whom HSPD-12 does not apply, D/As should follow appropriate Federal identity management guidance. Actor(s): mobile device app developer, mobile device app provider, mobile device manager, government agency, mobile device manufacturer.
- The threat connected with the use of digital certificates or OTPs is that the keys for access are stored on the device. Security for these keys/digital signatures (e.g., encryption, restricted access) is required to maintain the integrity of the authentication service. Additionally, an active revocation list (a CRL in digital certificate systems) is necessary, and the system must support checking the revocation list prior to completing the authentication. Additional vulnerabilities have been identified in some mobile platforms that enable compromise by allowing access to

[58] OMB M-04-04, E-authentication Guidance, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

[59] Telework Reference Architecture, version 1.0, paragraph 5.4.

[60] Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, March 24, 2011.

systems via screen unlock bypass.[61] Mitigations for this threat include strong unlock passwords/PINs and patches to correct system vulnerabilities. Actor(s): mobile device app developer, mobile device app provider, mobile device operating system developer, government agency.

- Additional issues include whether a mobile system supports multiple certificates for authentication vs. using a single certificate for all authentications (e.g., system access, VPN connectivity, email access, secure web access). Systems supporting only a single digital certificate may not be compatible with D/A systems that use separate certificates for access to different services. Actor(s): mobile device app developer, mobile device app provider mobile device operating system developer, government agency.

## B.7 User-Based Threats and Mitigations

User-based threats are exploits that arise from users internal to the enterprise. These exploits can be intentional or unintentional. Computer misuse and fraud are common intentional threats. User errors and negligence are common unintentional insider threats (e.g., divulging sensitive information as a result of social engineering efforts).

### B.7.1 Social Engineering

Social engineering is the art of manipulating people into performing actions or divulging confidential information. Phishing or spear phishing is a popular social engineering attack that involves sending what appears to be a legitimate message to deceive the user into providing a response and divulging sensitive information.[62]

#### Social Engineering Mitigation

- Social engineering threats can be mitigated through strong user training about social engineering threats and the risks posed to the user and the D/A enterprise by these attacks. Actor(s): mobile device consumer, government agency.

### B.7.2 Classified Information Spill

Classified information spills can occur through no fault of the user or the D/A. The Committee on National Security Systems (CNSS) maintains guidance on the interaction of classified material and mobile devices. For more information, see CNSS Policy No. 17, “National Information Assurance (IA) Policy on Wireless Capabilities”.[63]

[61] http://www.zdnet.com/blog/security/iphone-passcode-lock-bypass-vulnerability-again/7544.

[62] NASA. *Home Computer Security: A Guide for NASA HQ Personnel.* www.hq.nasa.gov/office/itcd/documents/home_computer_security_guide.docx.

[63] http://www.cnss.gov/Assets/pdf/CNSSP-17.pdf.

### Classified Information Spill Mitigation

- Develop, test, and document device cleaning procedures and train users and IT support staff on classified information spill procedures. Actor(s): mobile device consumer, government agency.

## B.7.3 Incident Involving Mobile Device Features

Incident responses involving mobile devices must be handled according to CNSS Policy.

### Incident Involving Mobile Device Mitigation

- Current incident response plans should be modified to address mobile devices. Actor(s): government agency

## B.7.4 Theft/Misuse of Services

An attacker or exploit may, without the enterprise's knowledge, use premium services that result in unexpected costs to enterprise. For example, malicious applications have been discovered that silently send premium text messages.

### Theft/Misuse of Services Mitigation

- Develop, test, and document the process to properly handle the device throughout its lifecycle: network access rules such as whether employees can connect to hotel or Wi-Fi networks, sanitizing a device after a classified message spill, checking device integrity after a potential compromise, or procedures to decommission a device. This information can be used to provide users with security awareness training on the threat posed by the theft or misuse of mobile device services. Furthermore, the theft or misuse of mobile device services can be addressed through the mitigations discussed in the section on Loss of Device. Actor(s): mobile device consumer, government agency.
- To minimize user-related risks, the D/A should use Configuration Profiles (if available) to enforce security policies. An administrator can specify a Configuration Profile to require an administrative password prior to erasing the profile, or explicitly locking the profile to the device such that its deletion will wipe all device content. Specifically, an administrator can both sign and encrypt configuration profiles to prevent modification or deletion of settings (Cryptographic Message Syntax, RFC 3852, is compatible with 3DES [Triple Data Encryption Standard] and AES [Advanced Encryption Standard] 128[64,65]). Actor(s): mobile device app developer, mobile device app provider, mobile device manager.

[64] Apple. "iPad in Business Security," Pg. 2, March 2011. http://www.apple.com/iphone/business/it-center/security.html.

[65] Apple. "Deploying iPhone and iPad Security Overview," Pg. 2. October 2011. https://ssl.apple.com/ca/ipad/business/docs/iOS_Security_Mar12.pdf.

### B.7.5 Non-GFE (Employee-Owned) Devices

D/As that allow employee-owned devices face additional security concerns. Users may accidentally purchase devices that are not genuine, and a clone may not possess the same security measures as the real product. Furthermore, sensitive data such as personally identifiable information may be vulnerable since users of employee-owned devices can download applications without restriction, including those that may place sensitive data on third-party servers. Use of non-GFE devices also increases the risk associated with classified/sensitive data, information leakage, and the associated loss of the user's property and the Government's data and information.

#### Non-GFE (Employee-Owned) Devices Mitigation

- D/As should prohibit employee-owned mobile devices purchased from unverified sources from accessing D/A enterprise assets. To encourage the use of authorized sources, D/As can sponsor an employee purchasing program.[66] Devices purchased under this program could be granted more privileged access. Actor(s): Mobile device consumer, government agency.
- Non-GFE devices should also be protected through features such as password protection and data wiping capability and the ability to locate lost or stolen devices through geolocation. Section 4.3 provides additional details and considerations for these capabilities. Actor(s): mobile device manager.

### B.7.6 Malicious Insider

An insider is anyone in an enterprise with approved access, privilege, or knowledge of information systems, services, and operations. A malicious insider is one motivated to adversely impact an enterprise through a range of actions that cause physical damage to hardware and/or that compromises information confidentiality, integrity, and/or availability.

#### Malicious Insider Mitigation

- To mitigate the threat of malicious insiders using mobile devices as the means for an attack, a D/A should implement access policies that limit the use of mobile device access to enterprise resources using administrator privileges and restrict management functions such as SSH from mobile devices. Actor(s): mobile device consumer, government agency.

### B.7.7 Tracking

The same features that help users to know their precise location for the purposes of navigation and theft-tracking can also provide that information to an adversary for malicious purposes. Illegitimate tracking can be performed through data mining and searches for records, pictures, or other geotagged data or examination and correlation of use patterns.

[66] Communications Security Establishment Canada. "Apple iPad Security and Best Practices." Updated October 31, 2011. www.cse-cst.gc.ca/its-sti/services/csg-cspc/csg-cspc30s-eng.html.

### Tracking Mitigation

- To mitigate the threat of mobile device tracking, the D/A should perform an analysis of the risks posed by tracking versus the benefits provided through the use of tracking. The use of third-party applications that use geolocation, which could lead to the tracking and storage of location data, should be minimized. Security policies should require the use of strong encryption methods for the storage or transmission of data between the device and the D/A MDM servers. Actor(s): mobile device app developer, mobile device app provider, mobile device manager, government agency, mobile device manufacturer.

## B.8 Service Provider-Based Threats and Mitigations

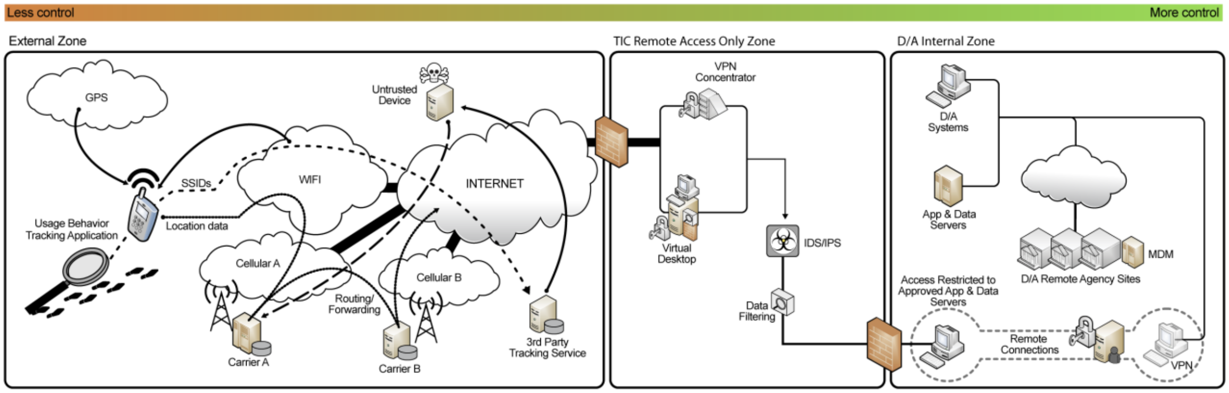

*Figure 16: Service Provider-based Threats*

Service-provider-based threats (Figure 16) are comprised of exploits that arise from the mobile carrier, targeting both the data and control planes of the mobile device. These exploits gain access to the carrier's management network to reconfigure the mobile device or to acquire sensitive data on the end device or cached at the carrier. Vulnerabilities also exist on other data channels besides traditional IP transport (such as MMS/SMS or management/control channel), which could be used to transfer viruses and worms.

OS-specific layered features and services offered and managed by the OS vendor can be another vector for exploitation, either by injecting a vulnerability or capturing sensitive data. Users might unintentionally opt-in for services such as backup, which may transport sensitive data into the vendor's cloud. While some vendors claim to encrypt user data, it is unclear what the strength of the encryption is or what the data removal process of the vendor is if the user decides eventually to opt-out.

There are many types of diagnostic data that can be used to correlate behavior of the user and/or the organization (e.g., local and remote logs). Some vendors also employ third-party software and services to combine geolocation with SSID information to provide the location of specific wireless networks, which is shared amongst their customers. It is unclear if the data is sent to the OS vendor first or to the third party. Other examples of third-party software installed by the OS vendor may be used to track user behavior as well as performance metrics. This data may also be sent directly to the vendor or to the third party.

Another threat source is the application service provider. Examples include application "storefronts" that are directly tied to the native operating system. The exploit may be directly embedded into the application, or it may unintentionally reconfigure the mobile device (directly or indirectly), or offer a service natively or through a third party, such as a chat service.

### B.8.1 Location Tracking

For years, carriers have been providing location services by passively capturing mobile device cellular signature data from the cell node and correlating it with the node's physical location. By correlating the mobile device signature with multiple node locations and using triangulation methods, location services have become much more accurate. Combining this data both with a local GPS receiver on the mobile device and with Wi-Fi location data, the accuracy and precision of the location of the mobile device can become quite high.

The management of location data is critical because it protects highly sensitive information about the location of mobile device owners as well as possible historical data that might predict patterns in their travels. Since the carrier manages and owns the cellular location data, it can be difficult to discover their management policies and practices, not to mention to review an audit. The OS and application vendors generate the GPS and Wi-Fi location data locally on the device, and in general it should be easier to manage, enforce, and audit its use.

If this data should be exposed to a covert entity, it could be disastrous for both the agency and the owner of the device. Actor(s): mobile device app developer, mobile device app provider, mobile device manager, government agency, mobile device manufacturer, mobile device cellular wireless carrier.

### B.8.2 Usage Behavior Tracking via Applications

Some third-party applications installed by the carrier, OS, or user, allows the tracking of selected events occurring on mobile devices. Although there has been a good deal of recent publicity surrounding possible invasion of device users' privacy by specific vendors,[67] contrary to some reports, it appears that most software is not capable of recording every action taken by a mobile user. Examples of some event types that can be tracked include:

- Recording which dialer buttons are pressed, to determine the destination of a phone call;
- Reporting GPS location data in some situations; and
- Recording the URLs that are being visited (including HTTPS resources), but not the contents of those pages, or other HTTP data.

Actor(s): mobile device app developer, mobile device app provider, mobile device manager.

[67] Rosenberg, Dan. "CarrierIQ: The Real Story." *It's Bugs All the Way Down.* December 5, 2011. http://vulnfactory.org/blog/2011/12/05/carrieriq-the-real-story/.

### B.8.3 Routing/Forwarding

Without an SLA with a carrier, it is extremely difficult to request a specific path of information flow from the mobile device through the carrier's infrastructure. It is almost impossible to request a path to the destination node because that path may include multiple carriers. While monitoring IP paths is possible via applications that are variants of the UNIX traceroute command, monitoring of voice and MMS/SMS paths is almost impossible. The carrier's data paths are dictated by business relationships and are subject to change based on contracts between carriers, link economics, link utilization, or link failure and recovery. When carrier administrative areas overlap, specifically along U.S. borders such as with Mexico and Canada, the path is subject to change and may use a provider, albeit an established multinational carrier that also operates within the U.S., that may have different security and privacy practices as well as different policies outside U.S. borders.

Because of the seemingly nondeterministic nature of routing/forwarding, it is best to treat all communication to and from the mobile device as if it were traversing multiple insecure networks. The encryption methods deployed should be end-to-end FIPS 140-2 approved or IPSec/SSL tunnels, so that all traffic is encrypted until the data can safely reach the intended environment. If a mobile device is not FIPS validated, D/As should not allow any transmission or processing of D/A-sensitive data. Until there is widespread adoption of FIPS 140-2, implementation and enforcement will be challenging at best. Actor(s): mobile device application developer, mobile device application provider.

### B.8.4 Data Ownership and Retention

Carriers own and manage many different types of mobile device data. The data types are highly diverse and include (but are not limited to) location, call records, IP flow records, configuration, identity, MMS/SMS messages, application logs, and email. It can be difficult to discover the carriers' management policies and practices, or to review an audit.

While it is possible to design and execute data ownership and retention SLA with a carrier, there are areas that are difficult, if not impossible, for the carrier to comply with. To reduce the risk of the loss of data ownership and management within the carriers' administrative domain, the following are best practices that should be adopted based on the business requirements, policies, and risks of the D/As:

- Treat all data channels to and from the device as insecure (e.g., IP, MMS/SMS, Voice);
- If possible, remove all sensitive data; if not possible, encrypt the data (of each "sandbox" as a whole or on a per file basis);
- Configure the device with non-D/A-specific identification parameters;
- Adopt virtualization and sandbox technologies to contain sensitive data; and
- Work closely with a carrier that understands data ownership and retention issues and provides a clear policy as well as an SLA for data management and retention.

Actor(s): mobile device application developer, mobile device application provider, mobile device cellular wireless carrier, mobile device manager, government agency, mobile device consumer.

# Appendix C Considerations for High-Risk Environments

The standards and practices in the preceding document are not intended to be a one-size-fits-all solution to the complex problems of securing mobile devices in Federal agencies. Simply put, some agencies and environments have lower risk tolerances than others. While this document is applicable to all Federal agencies, there are considerations (Figure 17) that are unique to the demands of agencies charged with security, police, and military operations, among others. The purpose of this appendix is to call out the security controls that are of special significance to D/As operating in these environments.

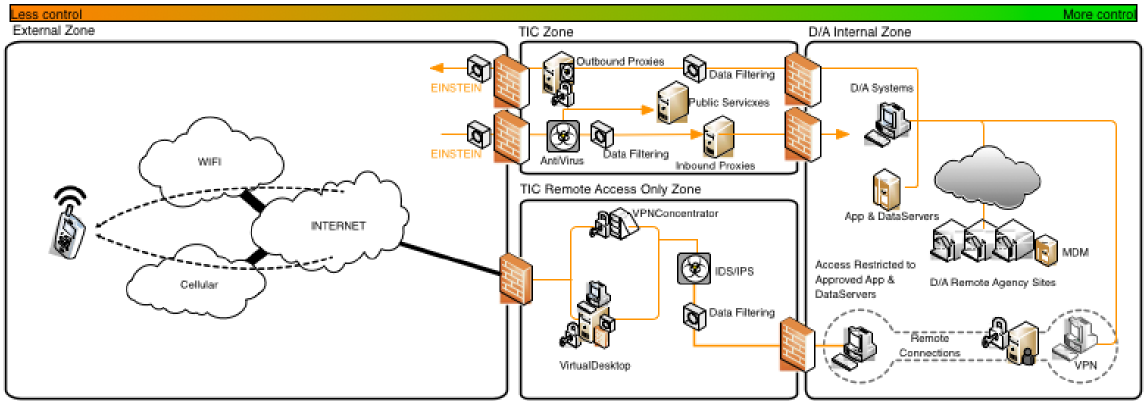

*Figure 17: High-Risk Environment Architecture Considerations*

1. Mobile Security Components

   a. Procurement and Provisioning Considerations

   Environments with minimal risk tolerance should avoid reliance on externally provided or configured equipment, and services and should exclusively deploy mobile devices as fully managed GFE as described in Section 3.2.1. In this configuration, the D/A controls the mobile service provider, mobile device hardware selection, operating system, and applications (including version control). In addition, features of the mobile device that will be enabled (e.g., camera, GPS, Bluetooth), storage controls, device disposal, and authentication techniques can also be provisioned and de-provisioned according to risk considerations.

   Additionally, control over device ownership allows the D/A to confiscate the device upon employee termination or reassignment, fully sanitize the stored information prior to disposal, determine the lifespan of the device in use, and clear the device’s memory contents in case of classified information spillage, without concern for the loss of the user’s personal information.

b. Network Segment Control and Approval

Ensure that mobile devices that are used in high-risk situations do not connect to multiple networks simultaneously, and assume that data and voice traversing over the mobile carrier's managed network can be intercepted and that the configuration and core components could be compromised via control plane channels. This assumption has strong implications in high-risk environments and must be taken into account when configuration policies and device profiles are created and tested.

Bluetooth personal area network connections provide native encryption and authentication mechanisms; however, there are well-known vulnerabilities and exploits[68] that discourage its use in high-risk environments.

One approach to minimizing the exposure of a mobile device to signal interception to mitigate the threat of data and voice collection over the air, is disabling 3/4G network capabilities in high-threat areas, such as foreign countries. Other mitigations include also disabling the Bluetooth, NFC, and 802.11 communications services, if no secure VPN services or features exist on the device.

Additionally, such devices can be required to use VPN services and features protected by strong network encryption and authentication techniques when accessing official network services.[69] Cloud connections should be restricted to a mutually authenticated FedRAMP-accredited cloud service provider and the security policy for mobile devices should also prohibit the dual connection to multiple networks, known as "split-tunneling."

High-risk Federal enterprises should use the 802.1x protocol for connection authentication, which allows network-capable devices to be integrated with a broad range of authentication environments.

c. Audits and Audit Trails

Audit trails maintain a record of system activity both by system and application processes and by user activity in systems and applications. Audit trails can also assist in detecting security violations, performance problems, and flaws in applications. Mobile devices in high-risk environments should at a minimum, log the time, date, and (where possible) geo-location of all network connections, login attempts and application accesses. Remote logging over unsecured networks should not be configured due to potential security issues, but devices should be configured to send remote logging data when connected to the known D/A infrastructure.

[68] NIST Special Publication 800-121, Guide to Bluetooth Security.
[69] NIST Special Publication 800-46, Guide to Enterprise Telework and Remote Access Security.

d. Authentication and Authorization

Authentication of mobile device users by the device operating system should be configured in all devices used in high-risk environments with special consideration given to the addition of two-factor authorization wherever possible. At present, third-party hardware solutions are becoming available that offer an additional layer of security to mobile devices and should be considered for deployment in high-risk environments.

e. Data Loss Prevention

Appropriate DLP measures for a mobile device in a high-risk environment include encrypting sensitive data according to the D/A's data at rest storage requirements. Every mobile device is itself a data store and must have the same or greater risk controls as those associated with the information stored on a stationary device.

On a mobile device, the ability to wipe data from a device that is lost or not under D/A control should be configured. Also, policy-based restrictions should be established on where a mobile device user can make copies of data available to the mobile device, on transmitting limited distribution data beyond authorized destinations, and on ensuring that data cannot be intercepted during transmission to or from the mobile device.

f. Encryption

For mobile security, strong encryption (FIPS 140-2) should protect the communication channels between the mobile device and the data and/or services to which the device will connect, as well as the data resident on the device. Encryption should be used to protect all forms of communication, including text messaging and voice communication where possible, and multiple layers of encryption (such as encrypted traffic flowing over a VPN) can be used to enhance the security posture even further.

g. Firewalls, access control lists, anti-malware systems and intrusion detection/prevention systems

Firewalls, access lists, anti-malware and IDS/IPS controls are generally not implemented directly on mobile devices at present. However, the D/A should use infrastructure-based systems between the mobile device and the D/A infrastructure to limit malicious traffic that attempts to enter the D/A from the mobile device.

h. Sandbox

Sandboxed applications on GFE mobile devices should be used even in high-risk environments to limit access to sensitive information. For example, file sharing applications with access to D/A sensitive information should be sandboxed to prevent data leakage or corruption.

**2.** High-risk Environment Mobile Security Functions

a. Management

Mobile security devices should be covered under existing D/A policy with respect to management authority and policy. NIST SP 800-53 outlines management controls appropriate to the Federal enterprise. The requirements for high-risk environments do not differ significantly from those outlined in Section 4, with the exception of special consideration being given to information access by mobile device administrators.

b. Training

Security training must be required for every network administrator and user. In high-risk environments, this training includes security awareness training to provide awareness of risks associated with the use of mobile devices and infrastructure technologies. The training security function should be supported by the policies and procedures developed as part of the management security function, but should include special attention to the selection of FIPS 140-2 algorithms where such selections are routinely made by users (such as VPN connection choices for example).

c. Physical Controls

Because mobile devices are designed to be carried about, physical controls of mobile devices themselves are largely a function of training. Users should be instructed not to leave devices unattended (even in locked cars, for example). However, physical controls must also be included for infrastructure-supporting mobile users as well. Routers, access points, and network endpoints must also be secured according to D/A security policy. Special consideration should be given to data stores used by mobile devices because these devices often contain a great deal of sensitive data.

d. Authentication

The authentication requirements of high-risk environments strongly favor the addition of a second factor for access to sensitive information. In addition, certain mobile devices can themselves be used as a second factor identification device that would necessarily bind them to D/A policy for the provision, use, and disposal of other access control devices.

e. Data Storage

As noted previously, user-available data stored on mobile devices must be stored with at least the same controls required for any other storage media. In high-risk environments, mobile-infrastructure diagnostic audit records (e.g., configuration, security, application, and system call log files) should be transferred to the MDM system in as near real time as possible and, if not, should be securely stored for later transmission.[70] After transfer, the data should be deleted from the device. Depending on the MDM and its configuration, the diagnostic log records may be extremely sensitive in nature.

f. Configuration

Configuration security in a high-risk environment poses some additional problems for a D/A beyond those of lower-risk environments. Generally speaking, D/A infrastructure teams must implement additional restrictions on data storage and transmission, which places greater demands on the MDM solution chosen. Policy use cases must be vetted to ensure that all security controls are in place, and mobile devices must be periodically checked by the MDM to monitor configuration consistency.

In addition, the control plane technology of the MDM must itself be monitored as a high-risk enterprise asset due to the sensitive nature of mobile device compromise; remote administration of the MDM should be disabled. In particular, cryptographic elements of a mobile infrastructure must be FIPS validated, and must follow agency policies with regard to key material storage, rotation, and destruction. Administrative access to mobile infrastructure devices must use multi-factor authentication.[71]

Agency-issued mobile devices must use authorized mobile communications methods exclusively, have enabled firewalls (e.g., IP, MMS/SMS, and Bluetooth),[72] have all unnecessary features disabled, and have anti-virus software with virus signatures that are updated frequently.

Filters should be employed to limit which applications have access to specific device resources such as the microphone, geolocation service, or other applications, such as the address book. Audit changes in configuration controls through continuous monitoring techniques, and transfer the audit records from the mobile device to the MDM as soon as possible. Near-real-time or periodic auditing is possible when a device has network connectivity, but audit information must be queued for transfer when connectivity is not possible. When disposing of a mobile infrastructure component, all sensitive configuration information, including data stored on the devices and passwords, is removed.

g. Secure Communications

[70] NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.

[71] NIST Special Publication 800-63, Electronic Authentication Guideline.

[72] NIST Special Publication 800-121, Guide to Bluetooth Security (draft).

Agencies operating mobile devices in high-risk environments must follow Federal encryption standards to protect agency data during access to information systems by users.[73]

Of particular sensitivity is the mobile device control plane that is part of the mobile infrastructure communication service. In high-risk environments, administration and network management of mobile infrastructure equipment must use strong multi-factor authentication and encryption for all communications.[74]

Furthermore, all cryptographic elements of a mobile infrastructure must be FIPS validated, and must follow agency policies with regard to key material storage, rotation, and destruction. The MDM must enforce, manage, and monitor the policies.

h. Traffic Inspection

Many of the characteristics associated with traffic inspection in a wired LAN, wireless LAN, and telework infrastructure apply to a mobile infrastructure. In high-risk environments, traffic from mobile devices to the D/A infrastructure should be monitored with the same granularity and frequency as laptop computers. Ideally, network traffic should be proxied through a D/A approved environment so that transactions may be securely monitored.

i. Packet Filtering

Special consideration must be given to ensure that the mobile infrastructure ingress from the internet is separated and segmented from internal D/A networks, and that traffic is restricted between the two networks. To accomplish this separation, stateful packet inspection should be combined with application packet filtering technologies where possible to maintain and monitor the boundaries between multi-tiered backend networks.[75]

j. Content Filtering

Agencies in high-risk environments must perform content filtering on all traffic entering or leaving the mobile infrastructure segment of their network to restrict the types of information that may be transferred between mobile clients and the enterprise.

k. Logging

D/A managers should integrate MDM functions with an SIEM infrastructure to monitor the collection, orchestration, and analysis of mobile device logging data. Some systems

[73] FIPS PUB 140-3 (Revised DRAFT 09/11/09) Security Requirements for Cryptographic Modules.

[74] NIST Special Publication 800-46, Guide to Enterprise Telework and Remote Access Security.

[75] NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.

collect a wide array of events in the network, system, application, and security domains, which provides a valuable tool for root cause analysis and reporting. Therefore, it is highly desirable that the SIEM system integrate tightly with the mobile device infrastructure, including the MDM.

l. Monitoring and Auditing

Periodic mobile system audits should be performed at least annually as a periodic evaluation of security. Mobile client devices and infrastructure components should be checked to ensure that they meet security configuration requirements, including authentication mechanisms, data encryption, and administrative access.

Monitoring the behavior of distributed mobile infrastructures and their users should be done in real time with anomalies transmitted to the CERT team. Mobile infrastructure security assessment in high-risk environments should include end-to-end operational verification of mobile client device services, configuration settings, review of audit logs, and relevant diagnostic information.

m. Response

In high-risk environments, incident response must include a remote wipe capability in addition to forensic auditing tools.

## Appendix D Acronyms

**3DES** – Triple Data Encryption Standard  
**A/D** – Analog-to-Digital  
**A-GPS** – Assisted Global Positioning System  
**AES** – Advanced Encryption Standard  
**BYOD –** Bring Your Own Device  
**CDMA** – Code Division Multiple Access  
**CMEA** – Cellular Message Encryption Algorithm  
**CVE** – Common Vulnerabilities and Exposures  
**CWE**- Common Weakness Enumeration  
**COPE** – Corporate Owned, Personally Enabled  
**D/A** – Department/Agency  
**DLP –** Data Loss Prevention  
**DRAM** – Dynamic Random Access Memory  
**EAP-FAST** – Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling  
**EAP-SIM** – Extensible Authentication Protocol for GSM Subscriber Identity Modules  
**EAP-TLS** – Extensible Authentication Protocol-Transport Layer Security  
**EAP-TTLS** – Extensible Authentication Protocol-Tunneled Transport Layer Security  
**EDGE** – Enhanced Data rates for GSM Evolution  
**EV-DO** – Evolution Data-Optimized  
**FedRAMP –** Federal Risk and Authorization Management Program  
**GFE** – Government Furnished Equipment  
**GPS** – Global Positioning System  
**GPRS** – General Packet Radio Service  
**GSM** – Global System for Mobile Communications  
**HSDPA** – High-Speed Downlink Packet Access  
**HSPD-12** – Homeland Security Presidential Directive 12  
**IAM** – Identity and Access Management  
**IDS** – Intrusion Detection System  
**IEEE** – Institute of Electrical and Electronics Engineers  
**IF** – Intermediate Frequency  
**IP** – Internet Protocol  
**IPS** – Intrusion Prevention System  
**IPSec** – Internet Protocol Security  
**L2TP** – Layer 2 Tunneling Protocol  
**LEAP** – Lightweight Extensible Authentication Protocol  
**MDM** – Mobile Device Management  
**MVNO** – Mobile Virtual Network Operator  
**NFC** – Near Field Communication  
**NIDS** – Network Intrusion Detection System  
**OS** – Operating System  
**OTP** – One-Time Password  
**PAN** – Personal Area Network  
**PDA** – Personal Digital Assistant  
**PEAP** – Protected Extensible Authentication Protocol  
**PKI** – Public Key Infrastructure  
**PPTP** – Point-to-Point Tunneling Protocol  
**QoS** – Quality of Service  
**RADIUS** – Remote Authentication Dial In User Service  
**RF** – Radio Frequency  
**S-MIME** – Secure Multipurpose Internet Mail Extension  
**SIEM** – Security Information and Event Management  
**SLA** – Service Level Agreement  
**SMS** – Short Message Service  
**SSID** – Service Set Identifier  
**SSL** – Secure Sockets Layer  
**TIC** – Trusted Internet Connection  
**UMTS** – Universal Mobile Telecommunications System  
**VDI** – Virtual Desktop Infrastructure  
**VLAN** – Virtual Local Area Network  
**VoIP** – Voice Over Internet Protocol  
**VPN** – Virtual Private Network

# Appendix E Glossary

| | |
|---|---|
| Audits and Audit Trails | Audits are conducted to support operational assurance and examine whether systems are meeting stated or implied security requirements, including system and organization policies.<br>Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.<br>Audit trails may be used as either a support for regular system operations, or as a kind of insurance policy, or as both of these. As insurance, audit trails are maintained but are not used unless needed, such as after a system outage. As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems. |
| Authentication and Authorization | Authentication is the process of verifying an identity. Electronic authentication (e-authentication) is the process of establishing confidence in identities electronically presented to an information system.[76]<br>Authentication precedes authorization. Authorization is the defining of privileges on a system. Authorization can be tied to identities or to roles and can control the actions of a user, executable code, or a data element, but authorization only succeeds if paired with authentication to validate which privileges should be assigned based on validating the identity being granted the privileges.<br>Mutual authentication is a higher level of authentication. In mutual authentication, both the authentication target and the authentication requestor verify the identity of the other end of the exchange. As an example, mutual authentication may occur between a user and a bank. The bank requires authentication of the requesting user to prove that the requestor should be granted access to a particular bank account. At the same time, the requesting users want proof that |

[76] NIST Special Publication 800-63-1, Electronic Authentication Guideline, December 2011.

| | |
|---|---|
| | they are connected to the actual bank web presence and not a "spoof" of the bank, to be sure they are not sharing their authentication credentials with a potential bad actor. |
| Control Plane | A control plane is a mechanism used to transmit control information from one system component to another. In the case of mobile devices, a control plane can have multiple forms. Wireless Carriers have a control plane built into the operating systems on their devices. The control plane uses specific message formats sent over the cellular network to cause specific behaviors on the mobile device. A MDM also uses a control plane, typically implemented as an IP network or cellular data connection to a device. |
| Data Loss Prevention | Data loss prevention (DLP) is the identification and safeguarding of information that should have controlled or limited distribution, that is, data that should not be in the public domain. Example data types that should be covered by data loss prevention efforts include (but are not limited to)<br>• Information formally classified by the U.S. Government as confidential, secret, or top secret;<br>• Information not formally classified, but which has been labeled for limited distribution (For Official Use Only, Sensitive But Unclassified, and similar terms);<br>• Information covered by the Privacy Act of 1974 or other Personally Identifiable Information (PII) designated as not for public release;<br>• Proprietary vendor information—information released by contractors and other entities to the Federal government for its internal use only.<br>DLP is the umbrella term used for efforts to ensure that limited distribution data is only available as authorized. Controls on limited distribution data include both data at rest (data temporarily or permanently stored in any way, including but not limited to physical drives and non-volatile or volatile memory), data in motion (data being transmitted within a device or between devices by any means), and data in processing (data being acted on by a process). |

| | |
|---|---|
| Encryption | Encryption is a cryptographic operation that is used to provide confidentiality for sensitive information; decryption is the inverse operation.[77] Encrypted data is inaccessible until decrypted, and the ability to decrypt can be limited only to authorized receivers of the data.<br>Encryption is used to protect data confidentiality; with additional features, it can also protect data integrity (through validating that the encrypted data has not been altered). Encryption can be used to protect data at rest and data in motion. |
| Firewalls, Access Control Lists, Anti-malware Systems and Intrusion Detection/Prevention Systems | Firewalls and access control lists use rules-based criteria to permit or deny communication based on rule sets defined by protocol standards and/or IT personnel. Firewalls and access lists work by evaluating communication passing through a security checkpoint (a physical or logical interface or other gateway) and permitting or denying traffic based on whether it meets or violates the configured rule sets.<br>Anti-malware systems and IDS/IPS systems perform functions similar to firewalls, with the distinction being that rather than being driven by static rule sets, these devices inspect data for malicious activity based on attack signatures. These signatures may look for malicious code in a data stream (anti-malware), or may look for malicious traffic patterns (IDS/IPS). A distinction between firewalls/access lists and anti-malware/IDS/IPS systems is that firewall and access list rule sets rarely need updating against new threats, while signature-based systems are continually adding new signatures to detect new attack vectors. |
| Container or Sandbox | A sandbox is a logical barrier that constrains the operation of code, data, and/or users within a defined area of a device.[78] Anything assigned to a sandbox has access to resources within the sandbox, but has controlled or no access to resources outside the sandbox. In this manner, activities within the sandbox are controlled to prohibit unintended interactions with resources outside the sandbox. |

[77] NIST Special Publication 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011.

[78] NIST Special Publication 800-28, Revision 2, Guidelines on Active Content and Mobile Code, March 2008.

| | |
|---|---|
| Virtual Private Networks (VPN) | A VPN is the application of encryption, data integrity, and authentication protocols to provide a secure connection between a D/A and a remote device or user. The authentication controls restrict the connection ability to only authorized users; the encryption controls ensure data confidentiality between the D/A and the remote device/user; the data integrity controls protect the data from modification during transit between the D/A and the remote user. When the data stream itself is also encrypted, the use of VPNs to send already-encrypted communications through an encrypted tunnel constitutes a form of double encryption. |

# Appendix F References

## DHS References

Telework Reference Architecture, U.S. Department of Homeland Security, National Cyber Security Division, Federal Network Security, Network & Infrastructure security, Oct 2011.

Trusted Internet Connections (TIC) Reference Architecture Document, U.S. Department of Homeland Security, Version 2.0, March 24, 2011.

## FBI References

"Safety and Security for the Business Professional Traveling Abroad," Federal Bureau of Investigation, February 23, 2012.

## FCC References

Electronic Code of Federal Regulations (e-CFR), Title 47 Telecommunication, Part 15 Radio Frequency Devices, March 22, 2012.

## NIST References

FIPS 140-1 and 140-2 Vendor List.

FIPS PUB 140-3 (Revised DRAFT 09/11/09) Security Requirements for Cryptographic Modules.

FIPS PUB 201 – Personal Identity Verification (PIV) of Federal Employees and Contractors.

Special Publication 500-292, NIST Cloud Computing Reference Architecture*,* September 2011

Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook, October 1995 (Chapters 9 and 18).

Special Publication 800-28, Revision 2, Guidelines on Active Content and Mobile Code, March 2008.

Special Publication - 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems.

NIST Special Publication - 800-41 – Guidelines on Firewalls and Firewall Policy.

Special Publication - 800-46 - Guide to Enterprise Telework and Remote Access Security.

Special Publication 800-48 R1 – Guide to Securing Legacy IEEE 802.11 Wireless Networks, Chapter 5 – Threats and Vulnerabilities.

Special Publication 800-53, Revision 4, Recommended Security Controls for Federal Information Systems, May 7, 2003 update.

Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography. August 2009, Page 48.

Special Publication 800-63-1, Electronic Authentication Guideline, December 2011.

Special Publication 800-121 – Guide to Bluetooth Security.

Special Publication 800-124: Guidelines on Cell Phone and PDA Security, Pg. 3-1, October 2008.

Special Publication 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011.

Special Publication 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.

### NASA References

Home Computer Security: A Guide for NASA HQ Personnel, National Aeronautics and Space Administration**.**

### NSA References

“Security Tips for Personally Managed Apple iPhones and iPads,” Pg. 1, March 2011.

### OMB References

M-04-04, E-authentication Guidance, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

M-11-11Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

### Subject Matter References

“Android Security Overview,” Google, March 2012.

“A Security-Driven Approach to Developing Mobile Solutions.” Threats for mobile devices derived from Bohne, Crossler, Field, Keppler, Carlson, McNab, Sheriff, and Sweitzer (The MITRE Corporation). September 8, 2011.

“Building Secure iPhone and iPad Apps.” Forrester, June 7, 2011.

“CarrierIQ: The Real Story, It’s Bugs All the Way Down,” Rosenberg, December 5, 2011.

“Deploying iPhone and iPad Security Overview,” Apple, Pg. 4, October 2011.

“Do Not Track”, Mozilla, February 23, 2012.

”Extensible Messaging and Presence Protocol,” IETF Network Working Group RFC 3920.

“IDC Report Says Smartphones Outsell Computers For the First Time,” GSMA Arena, February 9, 2011.

“iOS: Safari web settings.” Apple, Updated October 12, 2011.

“iPad in Business Security,” Apple, Pg. 5, March 2011.

“iPad in Business Security Overview,” Apple, Pg. 2, April 2011.

“iPhone Passcode lock Bypass Vulnerability Again,” ZDNet.

“Is Your Mobile Device Radiating Keys,” RSA 2012 Conference, MBS-401, March 2, 2012

Major Security Flaw Lets Anyone Bypass AT&T Samsung Galaxy S II Security.

Network Time Protocol: Best Practices White Paper, Cisco, document ID: 19643.

“Security Configuration Benchmark for iOS 4.3.3,” Version, Center for Internet Security, 1.3.0, Pg. 17, June 10, 2011.

State of Iowa Enterprise Mobile Device Security Standard, May 19, 2008.

## Whitehouse References

Homeland Security Presidential Directive-12 (HSPD-12), August 5, 2006.

Obama, Barack. United States Executive Office of the President, Executive Order No. 13571, Streamlining Service Delivery and Improving Customer Service April 27, 2011.

# Appendix G Policy Issues When Adopting Mobile Devices

Initiating an effort to create mobile device policies can be a complex task, given the multiple dimensions that must be considered, as well as the rapid evolution of the technology landscape. While the effort may seem daunting, establishing a good foundation with detailed use cases is essential to the effort's success. It is not the goal of this section to prescribe or suggest specific policies, but rather to offer additional perspectives by asking questions that a policy team may want to consider.

It is also not the intent of this section to promote a specific policy adoption framework or accompanying processes. There are many to choose from; each D/A must discover the process that best fits its organization.

While far from exhaustive, the following questions are meant to facilitate thought and discussion within D/As, as well as expose issues that the adoption of mobile devices can unearth. We assume that these questions are applicable if a non-GFE model is adopted, but have more complex and economically significant outcomes.

## G.1 Mobile Device Accreditation

- Will the mobile devices be included as part of the D/A computing infrastructure accreditation boundary?

## G.2 Mobile Device Acquisition

- Will there be a purchasing policy where only preapproved vendors are used? Is there a certification process for reapproving these vendors? How is this policy different for non-GFE hardware? How will this policy be enforced?
- Is there a baseline OS version that must be loaded before the device can be considered a candidate for management?
- Is there a minimum specific hardware configuration (DRAM, Flash)?

## G.3 Mobile Device Provisioning

- If the device is user-owned, should the D/A inspect it before permitting access to the infrastructure? Will the D/A inspect GFE or contractor company-owned devices (new) and if so, how extensively?
- Will ongoing (after initial adoption) enrollment of mobile devices in D/A MDM infrastructure be scheduled as batches or on-demand?

## G.4 Mobile Device Configuration, Monitoring, and Control

- Who will manage the device? The D/A IT staff, the user, or both?
- What maintenance tasks (such as software updates, data management, etc.) will be done on the device? What is the responsibility of the user? When will maintenance be done? What will the

proximity of the device be with respect to the D/A management infrastructure (approved VLANs)?

- Will the MDM employ a "poison pill" technology and, if so, what is the policy for its use?
- What MDM configuration management policies are needed (system configuration, access, integration into other monitoring infrastructures)?
- What is the data management policy for mobile device diagnostic data logs (monitoring, auditing, geolocation data, application usage data, MDM logs etc.)?
  - Who will have access to these logs?
  - What data will the MDM retain?
  - What use data will be kept (possibility aggregated) and for how long?
- Is tethering (packet forwarding) allowed and, if so, under what parameters?
- Does the user have the right to use the device for personal tasks?
- Is there a policy on what is strictly prohibited (applications, websites, etc.)?
- Must the user have a minimum set of geolocation services activated for monitoring purposes and to enable specific functionality?
- Data segmentation
  - With respect to user-owned devices, if the user uses applications that are not approved by the agency for official D/A work, what is the mechanism for detecting their use and for enforcing the policy?
  - What is the policy for contact list sharing between applications?
- Can users download their own applications?
  - If so, is there a restriction on the source and the application type?
  - How will such a policy be monitored and enforced?
- What is the policy regarding which applications are restricted? If the D/A discovers a restricted application, what is the mitigation process as the result of the discovery?

## G.5 Mobile Device Service Management

- Will there be any D/A-owned data that resides directly on the device and, if so, how will it be managed? How will it be discovered? Will there be periodic audits? How will audit violations be enforced?
- Can the user use other types of backup services (e.g., cloud, syncing to a local device) and, if so, for what types of data on the device? How will the policy be enforced?
- What is the policy for managing enterprise application stores?
  - Who will have access and have the capabilities to publish and rescind applications?
  - How will these staff members be audited?
  - What is the policy for software acceptance as well as revocation?
- Must the device use the approved D/A's VPN/TIC service for all communications or only for official D/A work? How does device ownership and procurement affect the use of the VPN/TIC service?

- Will data roaming be permitted, and, if so, under what carriers? Outside the U.S.? With multinational/international carriers near U.S. borders? How will this restriction be enforced?
- Will there be a data use policy where the user is required to stay under a specific monthly limit (GB/month)? What is the policy for enforcement? How does the user know what their current use is in relation to the policy?
- What is the policy for peer-to-peer communication and how is it enforced?
- Will the device or specific applications have restricted use depending on the location of the end-user device (e.g., out of the country, tied to a specific carrier)?
- Must the user download only applications and documents from D/A sponsored and managed application stores and repositories?
- If D/As are developing applications internally, what acceptance policies will be adopted for conformance?
  - Internal or third-party code review?
  - Obfuscation review of critical modules (RSA)?
  - RF data loss review by third party?
  - Third-party penetration tests?
  - Operational review for application management and data trail access?

## G.6 Mobile Device Security Management

- Will the D/A monitor and audit the device and to what level?
- Can the D/A revoke the use of the device at any time and if so, at what level of service?
- Must the device make contact with the D/A's infrastructure for management purposes on a periodic basis, and if so, will there be a suspension of service if the period between contacts is too great?
- What is the policy for recommending, requiring, or approving specific ancillary devices (e.g., crypto, authentication, Bluetooth headsets)?
- What is the authentication/authorization policy and what are its methods of enforcement?
- What level of encryption will be used for communications with the D/A? Will it be the same for all communications, or defined on a case-by-case or application-by-application basis?
- Will voice encryption be required, and, if so, what is the use scenario?

## G.7 Mobile Device Expense Management

- Can the user use local "hot spots" or other non-D/A managed Wi-Fi infrastructures, such as a network at the user's own residence?

## G.8 Mobile Device Customer Care

- What user training and awareness programs will be put into place?
  - Are they mandatory for all staff or only mobile device users?
  - How often must users retake the training?

  - What form will the training take (e.g., instructor led, computer based, and/or written)?
  - Who will prepare/update the content and determine user proficiency levels?
  - Is the training required to be current for users to remain connected to D/A data from mobile platforms?
- What is the policy for sharing with users their usage pattern over time?
- Who can use the end user's device and to what capacity?
  - Other D/A members of the same organization, and, if so, at what level of service?
  - Family members, and, if so, under what circumstances (e.g., emergency, expediency)?
- Will the D/A provide technical support for all mobile devices accessing D/A data? Is this support limited only to GFE provided devices? If not, how will this support be limited?

## G.9 Mobile Device Retirement and Reuse

- Can the mobile device be reassigned to a different user when the initial user no longer requires access?
- What is the policy concerning the disposition of the mobile device upon retirement? Will it be reallocated, destroyed, recycled, or stored?
- Who determines when a device is no longer supported or allowed to access D/A resources?

# Appendix H Acknowledgments

This document is the product of an ongoing multi-agency collaboration to provide guidance for the successful implementation of mobile device infrastructures at Federal civilian agencies. Participants from several agencies have graciously volunteered their expertise, and this document would not be possible without their selfless contributions.  Departments and agencies that contributed to the development of the mobile security reference architecture are listed below.

| Agencies Contributing to the Development of the MSRA | | | |
|---|---|---|---|
| ATF | CDC | CMS | DHS |
| DNI | DOD | DOI | DOJ |
| DOL | ED | EPA | FAA |
| FBI | FDIC | FERC | FRB |
| GSA | HHS | HUD | IRS |
| NASA | NGS | NIH | ODNI |
| RRB | TREAS | USAID | USDA |
| USPS | VA | WHMO | |

## Architecture Document Team Members

| Name | Organization |
|---|---|
| **David Carroll** | Department of Homeland Security- Office of the Chief Information Officer |
| **Marilyn Rose** | Department of Homeland Security (Project Leader) |
| **Vincent Sritapan** | Department of Homeland Security- Office of the Chief Information Officer |