National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-124
Revision 1 (Draft)

Guidelines for Managing and Securing Mobile Devices in the Enterprise (Draft)

Recommendations of the National Institute of Standards and Technology

Murugiah Souppaya
Karen Scarfone

NIST Special Publication 800-124
Revision 1 (Draft)

Guidelines for Managing and Securing Mobile Devices in the Enterprise (Draft)

Recommendations of the National Institute of Standards and Technology

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

Karen Scarfone
Scarfone Cybersecurity

C O M P U T E R S E C U R I T Y

July 2012

U.S. Department of Commerce

Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology

Patrick D. Gallagher, Under Secretary of Commerce
for Standards and Technology and Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-124 Revision 1 (Draft)
Natl. Inst. Stand. Technol. Spec. Publ. 800-124 rev. 1, 29 pages (July 2012)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *July 10* through *August 17, 2012*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: 800-124comments@nist.gov

Acknowledgments

The authors, Murugiah Souppaya of the National Institute of Standards and Technology (NIST) and Karen Scarfone of Scarfone Cybersecurity, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content, including Tom Karygiannis of NIST. The authors especially appreciate the contributions of Wayne Jansen, who co-authored the original version of this publication. Additional acknowledgments will be added to the final version of the publication.

Section 4 of this publication is based on Section 4 of NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices* [SP800-111] by Karen Scarfone, Murugiah Souppaya, and Matt Sexton.

Abstract

Mobile devices, such as smart phones and tablets, typically need to support multiple security objectives: confidentiality, integrity, and availability. To achieve these objectives, mobile devices should be secured against a variety of threats. The purpose of this publication is to help organizations centrally manage and secure mobile devices. Laptops are out of the scope of this publication, as are mobile devices with minimal computing capability, such as basic cell phones. This publication provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use and provides recommendations for securing mobile devices throughout their life cycles. The scope of this publication includes securing both organization-provided and personally-owned (bring your own device) mobile devices.

Keywords

cell phone security; information security; mobile device security; remote access; telework

Trademarks

Table of Contents

Executive Summary ..... **vi**

1. Introduction **1**

1.1 Purpose and Scope 1
1.2 Audience 1
1.3 Document Structure 1

2. Mobile Device Overview **2**

2.1 Defining Mobile Device Characteristics 2
2.2 High-Level Threats and Vulnerabilities 3
2.2.1 Lack of Physical Security Controls 3
2.2.2 Use of Untrusted Mobile Devices 4
2.2.3 Use of Untrusted Networks 4
2.2.4 Use of Applications Created by Unknown Parties 4
2.2.5 Interaction with Other Systems 5
2.2.6 Use of Untrusted Content 5
2.2.7 Use of Location Services 6

3. Technologies for Mobile Device Management **7**

3.1 Components and Architectures 7
3.2 Capabilities 8

4. Security for the Enterprise Mobile Device Solution Life Cycle **10**

4.1 Initiation 10
4.1.1 Restrictions on Mobile Devices and Access Levels 11
4.1.2 Additional User Requirements 12
4.2 Development 12
4.3 Implementation 13
4.4 Operations and Maintenance 14
4.5 Disposal 15

Appendix A— Supporting NIST SP 800-53 Security Controls and Publications **16**

Appendix B— Acronyms and Abbreviations **19**

Appendix C— Resources **20**

Executive Summary

Mobile devices typically need to support multiple security objectives: confidentiality, integrity, and availability. To achieve these objectives, mobile devices should be secured against a variety of threats. General security recommendations for any IT technology are provided in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* [SP800-53]. Specific recommendations for securing mobile devices are presented in this publication and are intended to supplement the controls specified in SP 800-53.

This publication provides recommendations for securing particular types of mobile devices, such as smart phones and tablets. Laptops are specifically excluded from the scope of this publication because the security controls available for laptops today are quite different than those available for smart phones, tablets, and other mobile device types. Mobile devices with minimal computing capability, such as basic cell phones, are also out of scope because of the limited security options available and the limited threats they face.

Centralized mobile device management technologies are a growing solution for controlling the use of both organization-issued and personally-owned mobile devices by enterprise users. In addition to managing the configuration and security of mobile devices, these technologies offer other features, such as providing secure access to enterprise computing resources. There are two basic approaches to centralized mobile device management: use a messaging server's management capabilities (sometimes from the same vendor that makes a particular brand of phone), or use a product from a third party, which is designed to manage one or more brands of phone. It is outside the scope of this publication to provide any recommendations for one approach over the other; both approaches can provide the necessary centralized management functionality.

Organizations should implement the following guidelines to improve the security of their mobile devices.

Organizations should develop system threat models for mobile devices and the resources that are accessed through the mobile devices.

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices (for example, desktop and laptop devices only used within the organization's facilities and on the organization's networks). Before designing and deploying mobile device solutions, organizations should develop system threat models. Threat modeling involves identifying resources of interest and the feasible threats, vulnerabilities, and security controls related to these resources, then quantifying the likelihood of successful attacks and their impacts, and finally analyzing this information to determine where security controls need to be improved or added. Threat modeling helps organizations to identify security requirements and to design the mobile device solution to incorporate the controls needed to meet the security requirements.

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

Most organizations do not need all of the possible security services provided by mobile device solutions. Categories of services to be considered include the following:

- **General policy:** enforcing enterprise security policies on the mobile device, such as restricting access to hardware and software, managing wireless network interfaces, and automatically monitoring and reporting when policy violations occur.

- **Data communication and storage:** supporting strongly encrypted data communications and data storage, and remotely wiping the device if it is lost or stolen and is at risk of having its data recovered by an untrusted party.
- **User and device authentication:** requiring authentication before accessing organization resources, resetting forgotten passwords remotely, automatically locking idle devices, and remotely locking devices suspected of being left unlocked in an unsecured location.
- **Applications:** restricting which applications may be installed (through whitelisting or blacklisting), installing and updating applications, restricting the use of synchronization services, digitally signing applications, distributing the organization's applications from a dedicated mobile application store, and limiting or preventing access to the enterprise based on the mobile device's operating system version or mobile device management software client version.

Organizations should have a mobile device security policy.

A mobile device security policy should define which types of mobile devices are permitted to access the organization's resources, the degree of access that various classes of mobile devices may have—for example, organization-issued devices versus personally-owned (bring your own device) devices—and how provisioning should be handled. It should also cover how the organization's centralized mobile device management servers are administered and how policies in those servers are updated. The mobile device security policy should be documented in the system security plan. To the extent feasible and appropriate, the mobile device security policy should be consistent with and complement security policy for non-mobile systems.

Organizations should implement and test a prototype of their mobile device solution before putting the solution into production.

Aspects of the solution that should be evaluated for each type of mobile device include connectivity, protection, authentication, application functionality, solution management, logging, and performance. Another important consideration is the security of the mobile device implementation itself; at a minimum, all components should be updated with the latest patches and configured following sound security practices. Also, use of jailbroken or rooted phones should be automatically detected when feasible. Finally, implementers should ensure that the mobile device solution does not unexpectedly "fall back" to default settings for interoperability or other reasons.

Organizations should fully secure each organization-issued mobile device before allowing a user to access it.

This ensures a basic level of trust in the device before it is exposed to threats. For any already-deployed organization-issued mobile device with an unknown security profile (e.g., unmanaged device), organizations should recover them, restore them to a known good state, and fully secure them before returning them to their users.

Organizations should regularly maintain mobile device security.

Helpful operational processes for maintenance include checking for upgrades and patches, and acquiring, testing, and deploying them; ensuring that each mobile device infrastructure component has its clock synced to a common time source; reconfiguring access control features as needed; and detecting and documenting anomalies within the mobile device infrastructure. Also, organizations should periodically perform assessments to confirm that their mobile device policies, processes, and procedures are being

followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing.

1. Introduction

1.1 Purpose and Scope

The purpose of this publication is to help organizations centrally manage and secure mobile devices, such as smart phones and tablets. (Laptops are out of the scope of this publication, as are mobile devices with minimal computing capability, such as basic cell phones.) This publication provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use and provides recommendations for securing mobile devices throughout their life cycles.

The scope of this publication includes both organization-provided and personally-owned (bring your own device) mobile devices.

1.2 Audience

This document is intended for security managers, engineers, administrators, and others who are responsible for planning, implementing, and maintaining the security of mobile devices. It assumes that readers have a basic understanding of mobile device technologies and enterprise security principles.

1.3 Document Structure

The remainder of this document is organized into the following sections and appendices:

- Section 2 provides an overview of mobile devices, focused on what makes them different from other computing devices, particularly in terms of security risk.
- Section 3 presents an introduction to technologies for centralized mobile device management.
- Section 4 discusses security throughout the mobile device life cycle. Examples of topics addressed in this section include mobile device security policy creation, design and implementation considerations, and operational processes that are particularly helpful for security.
- Appendix A lists the major controls from NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* that affect enterprise mobile device security.
- Appendix B provides an acronym and abbreviation list.
- Appendix C lists resources that may be useful for gaining a better understanding of mobile device security.

2. Mobile Device Overview

This section gives an overview of mobile devices, such as smart phones and tablets. Laptops are specifically excluded from the scope of this publication because the security controls available for laptops today are quite different than those available for smart phones, tablets, and other mobile device types. Mobile devices with minimal computing capability, such as basic cell phones, are also out of scope because of the limited security options available and the limited threats they face.

This section discusses the features of mobile devices, focusing on what makes mobile devices different from other computing devices, particularly in terms of security risk. This section also presents high-level recommendations for mitigating the risks that these mobile devices currently face.

2.1 Defining Mobile Device Characteristics

Mobile device features are constantly changing, so it is difficult to define the term "mobile device". However, as features change, so do threats and security controls, so it is important to establish a baseline of mobile device features. The following hardware and software characteristics collectively define the baseline for the purposes of this publication:

- A small form factor
- At least one wireless network interface for Internet access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with Internet connectivity.
- Local built-in (non-removable) data storage
- An operating system that is not a full-fledged desktop or laptop operating system
- Applications available through multiple methods (provided with the operating system, accessed through web browser, acquired and installed from third parties)
- Built-in features for synchronizing local data with a remote location (desktop or laptop computer, organization servers, telecommunications provider servers, other third party servers, etc.)

The list below details other common, but optional, characteristics of mobile devices. These features do not define the scope of devices included in the publication, but rather indicate features that are particularly important in terms of security risk. This list is not intended to be exhaustive, and is merely illustrative of common features of interest as of this writing.

- Network services:
  - One or more wireless personal area network interfaces, such as Bluetooth or near-field communications
  - One or more wireless network interfaces for voice communications, such as cellular
  - Global Positioning System (GPS), which enables location services
- One or more digital cameras
- Microphone

- Storage:
  - Support for removable media
  - Support for using the device itself as removable storage for another computing device

2.2 High-Level Threats and Vulnerabilities

Mobile devices typically need to support multiple security objectives. These can be accomplished through a combination of security features built into the mobile devices and additional security controls applied to the mobile devices and other components of the enterprise IT infrastructure. The most common security objectives for mobile devices are as follows:

- Confidentiality—ensure that transmitted and stored data cannot be read by unauthorized parties
- Integrity—detect any intentional or unintentional changes to transmitted and stored data
- Availability—ensure that users can access resources using mobile devices whenever needed.

To achieve these objectives, mobile devices should be secured against a variety of threats. General security recommendations for any IT technology are provided in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* [SP800-53].[1] Specific recommendations for securing mobile devices are presented in this publication and are intended to supplement the controls specified in SP 800-53. See Appendix A of this document for a summary of SP 800-53 controls most closely related to mobile device security.

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices (e.g., desktop and laptop devices only used within the organization's facilities and on the organization's networks). Before designing and deploying mobile device solutions, organizations should develop system threat models for the mobile devices and the resources that are accessed through the mobile devices. Threat modeling involves identifying resources of interest and the feasible threats, vulnerabilities, and security controls related to these resources, then quantifying the likelihood of successful attacks and their impacts, and finally analyzing this information to determine where security controls need to be improved or added. Threat modeling helps organizations to identify security requirements and to design the mobile device solution to incorporate the controls needed to meet the security requirements. Major security concerns for these technologies that would be included in most mobile device threat models are listed below.

2.2.1 Lack of Physical Security Controls

Mobile devices are typically used in a variety of locations outside the organization's control, such as employees' homes, coffee shops, hotels, and conferences. Even mobile devices only used within an organization's facilities are often transported from place to place within the facilities. The devices' mobile nature makes them much more likely to be lost or stolen than other devices, so their data is at increased risk of compromise. When planning mobile device security policies and controls, organizations should assume that mobile devices will be acquired by malicious parties who will attempt to recover sensitive data either directly from the devices themselves or indirectly by using the devices to access the organization's remote resources.

[1] These recommendations are linked to three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system, as defined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* [FIPS199].

The mitigation strategy for this is layered. One layer involves protecting sensitive data—either encrypting the mobile device's storage so that sensitive data cannot be recovered from it by unauthorized parties, or not storing sensitive data on mobile devices. Even if a mobile device is always in the possession of its owner, there are other physical security risks, such as an attacker looking over a teleworker's shoulder at a coffee shop and viewing sensitive data on the mobile device's screen (for example, a password being entered). A second mitigation layer involves requiring authentication before gaining access to the mobile device or the organization's resources accessible through the device. A mobile device usually has a single authenticator—not a separate account for each user of the device—as it is assumed that the device only has one user. So there is no username, just a password, which is often a PIN. More robust forms of authentication, such as domain authentication, can be used instead of or in addition to the built-in device authentication capabilities.

2.2.2 Use of Untrusted Mobile Devices

Many mobile devices, particularly those that are personally owned (bring your own device, BYOD), are not necessarily trustworthy. Current mobile devices lack the root of trust features (e.g., TPMs) that are increasingly built into laptops and other types of hosts. There is also frequent jailbreaking and rooting of mobile devices, which means that the built-in restrictions on security, operating system use, etc. have been bypassed. Organizations should assume that all phones are untrusted unless the organization has properly secured them before user access and monitors them continuously while in use with enterprise applications or data.

There are several additional possible mitigation strategies related to use of untrusted mobile devices. One option is to restrict or prohibit use of BYOD devices, thus favoring organization-issued devices. Another effective technique is to fully secure each organization-issued phone before allowing it to be used; this gets the phone in as trusted a state as possible when initially deployed, and deviations from this secure state can be monitored and addressed. There are also technical solutions for achieving degrees of trust, such as running the organization's software in a secure, isolated sandbox on the phone, or using device integrity scanning applications.

2.2.3 Use of Untrusted Networks

Because mobile devices primarily use non-organizational networks for Internet access, organizations normally have no control over the security of the external networks the devices use. Communications systems may include broadband networks, such as cable, and wireless mechanisms such as Wi-Fi and cellular networks. These communications systems are susceptible to eavesdropping, which places sensitive information transmitted at risk of compromise. Man-in-the-middle attacks may also be performed to intercept and modify communications. Unless it is absolutely certain that the mobile device will not be used on any networks not controlled by the organization or any other untrusted networks, organizations should plan their mobile device security on the assumption that the networks between the mobile device and the organization cannot be trusted.

Risk from use of unsecured networks can be reduced by using strong encryption technologies to protect the confidentiality and integrity of communications, as well as using mutual authentication mechanisms to verify the identities of both endpoints before transmitting data.

2.2.4 Use of Applications Created by Unknown Parties

Mobile devices are designed to make it easy to find, acquire, install, and use third-party applications. This poses obvious security risks, especially for mobile device platforms that do not place security restrictions or other limitations on third-party application publishing. Organizations should plan their mobile device

security on the assumption that unknown third-party mobile device applications downloadable by users should not be trusted.

Risk from these applications can be reduced in several ways, such as prohibiting all installation of third-party applications, implementing whitelisting to prohibit installation of all unapproved applications, or implementing a secure sandbox that isolates the organization's data and applications from all other data and applications on the mobile device. Another general recommendation is to perform a risk assessment on each third-party application before permitting its use on the organization's mobile devices.

It is important to note that even if these mitigation strategies are implemented for third-party applications, users can still access untrusted web-based applications through browsers built into their mobile devices. The risks inherent in this can be reduced by prohibiting or restricting browser access, or by using a separate browser within a secure sandbox for all browser-based access related to the organization, leaving the mobile device's built-in browser for other uses.

2.2.5 Interaction with Other Systems

Mobile devices may interact with other systems in terms of data synchronization and storage. Local system interaction generally involves connecting a mobile device to a desktop or laptop via a cable for charging and/or syncing. Remote system interaction most often involves automatic backups of data to a cloud-based storage solution. When all of these components are under the organization's control, risk is generally acceptable, but often one or more of these components are external. Examples include attaching a personally-owned mobile device to an organization-issued laptop, attaching an organization-issued mobile device to a personally-owned laptop, and attaching an organization-issued mobile device to a remote backup service. In all of these scenarios, the organization's data is at risk of being stored in an unsecured location outside the organization's control; transmission of malware from device to device is also a possibility.

The mitigation strategies depend on the type of attachment. Preventing an organization-issued mobile device from syncing with a personally-owned computer necessitates security controls on the mobile device that restrict what devices it can synchronize with. Preventing a personally-owned mobile device from syncing with an organization-issued computer necessitates security controls on the organization-issued computer, restricting the connection of mobile devices. Finally, preventing the use of remote backup services can possibly be achieved by blocking use of those services (e.g., not allowing the domain services to be contacted) or by configuring the mobile devices not to use such services.

2.2.6 Use of Untrusted Content

Mobile devices may use untrusted content that other types of devices generally do not encounter. An example is Quick Response (QR) codes. They are specifically designed to be viewed and processed by mobile device cameras. Each QR code is translated to a URL, so malicious QR codes could direct mobile devices to malicious websites. This could allow for targeted attacking, such as placing malicious QR codes at a location where targeted users gather.

A primary mitigation strategy is to educate users on the risks inherent in untrusted content and to discourage users from accessing untrusted content with any mobile devices they use for work. It is also possible to restrict peripheral use on mobile devices, such as disabling camera use in order to prevent QR codes from being processed.

2.2.7 Use of Location Services

Mobile devices with GPS capabilities typically run what are known as location services. These services map a GPS-acquired location to the corresponding businesses or other entities close to that location. Location services are heavily used by social media, navigation, web browsers, and other mobile-centric applications. In terms of organization security, mobile devices with location services enabled are at increased risk of targeted attacks because it is easier for potential attackers to determine where the user and the mobile device are, and to correlate that information with other sources about who the user associates with and the kinds of activities they perform in particular locations

This situation can be mitigated by disabling location services or by prohibiting use of location services for particular applications such as social networking or photo applications. Users may also be trained to turn off location services when in sensitive areas. However, a similar problem can occur even if GPS capabilities or location services are disabled. It is increasingly common for websites and applications to determine a person's location based on their Internet connection, such as a Wi-Fi hotspot or IP address range. The primary mitigation for this is to opt out of location services whenever possible.

3. Technologies for Mobile Device Management

Centralized mobile device management technologies are a growing solution for controlling the use of both organization-issued and personally-owned mobile devices by enterprise users. In addition to managing the configuration and security of mobile devices, these technologies offer other features, such as providing secure access to enterprise computing resources. This section provides an overview of the current state of these technologies, focusing on the technologies' components, architectures, and capabilities.

3.1 Components and Architectures

There are two basic approaches to centralized mobile device management: use a messaging server's management capabilities (often from the same vendor that makes a particular brand of phone), or use a product from a third party, which is designed to manage one or more brands of phone. It may be possible with the latter approach to have a single product that can manage multiple brands of phones desired for use within an enterprise. However, a product provided by a phone manufacturer may have more robust support for the phones than third party products. It is outside the scope of this publication to recommend one approach over the other; both approaches can provide the necessary centralized management functionality.

Architecturally, both approaches to centralized mobile device management are quite similar. The typical solution has a straightforward client/server architecture. The enterprise contains one or more servers that provide the centralized management capabilities, and one or more client applications are installed on each mobile device[2] and configured to run in the background at all times. If the device is organization issued, the client application typically manages the configuration and security of the entire device. If the device is BYOD, the client application typically manages only the configuration and security of itself and its data, not the entire device. The client application and data are essentially sandboxed from the rest of the device's applications and data, both helping to protect the enterprise from a compromised device and helping to preserve the privacy of the device's owner.

The centralized mobile device management may make use of other enterprise services, such as domain authentication services and virtual private networking (VPN) services. See Section 3.2 for additional information.

If there is not a centralized management solution, or certain mobile devices cannot use it, then mobile devices have to be managed individually and manually. In addition to the additional resources expended, there are two major security problems with this:

- The security controls provided by a mobile device often lack the rigor of those provided by a centralized mobile device management client application. For example, a mobile device often supports only a short passcode for authentication and may not support strong storage encryption. This will necessitate acquiring, installing, configuring, and maintaining a variety of third-party security controls that provide the missing functionality.
- It may not be possible to manage the security of the device when it is not physically present within the enterprise. It is possible to install utilities that manage devices remotely, but it will require significantly more effort to use such utilities to manually apply updates and perform other maintenance and management tasks with out-of-office mobile devices.

[2] The client applications may have been preinstalled by the vendor.

3.2 Capabilities

This section describes security services commonly provided for mobile devices. These services apply to the entire mobile device (if it is wholly managed) or to the mobile device's secure sandbox (as explained in Section 3.1), unless explicitly noted otherwise. These services are equally relevant for centrally managed or individually managed mobile devices.

Most organizations will not need all of the security services listed in this section. Organizations deploying mobile devices should consider the merits of each security service, determine which services are needed for their environment, and then design and acquire one or more solutions that collectively provide the necessary services.

1. **General policy.** The centralized technology can enforce enterprise security policies on the mobile device, including (but not limited to) other policy items listed throughout Section 3.2. General policy restrictions of particular interest for mobile device security include the following:

   - Restrict user and application access to hardware, such as the digital camera, GPS, Bluetooth interface, USB interface, and removable storage.
   - Restrict user and application access to the built-in web browser, email client, application installation services, etc.
   - Manage wireless network interfaces (Wi-Fi, Bluetooth, etc.)
   - Automatically monitor, detect, and report when policy violations occur.

2. **Data Communication and Storage**

   - Strongly encrypt data communications between the mobile device and the organization. This is most often in the form of a VPN, although it can be established through other uses of encryption.
   - Strongly encrypt stored data on both built-in storage and removable media storage. Removable media can also be "bound" to particular devices such that encrypted information can only be decrypted when the removable media is attached to the device, thereby mitigating the risk of offline attacks on the media.
   - Remotely wipe the device (to scrub its stored data) if it is suspected that the device has been lost, stolen, or otherwise fallen into untrusted hands and is at risk of having its data recovered by an untrusted party. A device often can also be configured to wipe itself after a certain number of incorrect authentication attempts.

3. **User and Device Authentication**

   - Require a password/passcode and/or other authentication (e.g., domain authentication) before accessing the organization's resources. This includes basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out the account, wiping the device).
   - If device account lockout is enabled or the device password/passcode is forgotten, an administrator can reset this remotely to restore access to the device.
   - Have the device automatically lock itself after it is idle for a period (e.g., 5 minutes).

- Remotely lock the device, if it is suspected that the device has been left in an unlocked state in an unsecured location.

4. Applications

- Restrict which applications may be installed through whitelisting (preferable) or blacklisting.
- Install, update, and remove applications.
- Restrict the use of synchronization services (e.g., local device synchronization, remote synchronization services and websites).
- Digitally sign applications to ensure that only applications from trusted entities are installed on the device and that code has not been modified.
- Distribute the organization's applications from a dedicated mobile application store.
- Limit or prevent access to the enterprise based on the mobile device's operating system version (including whether the device has been rooted/jailbroken) or its mobile device management software client version (if applicable). Note that this information may be spoofable.

4. Security for the Enterprise Mobile Device Solution Life Cycle

This section explains how the concepts presented in the previous sections of the guide should be incorporated throughout the entire life cycle of enterprise mobile device solutions, involving everything from policy to operations. The section references a five-phase life cycle model to help organizations determine at what point in their mobile device solution deployments a recommendation may be relevant. Organizations may follow a project management methodology or life cycle model that does not directly map to the phases in the model presented here, but the types of tasks in the methodology and their sequencing are probably similar. The phases of the life cycle are as follows:

- **Phase 1: Initiation.** This phase involves the tasks that an organization should perform before it starts to design a mobile device solution. These include identifying needs for mobile devices, providing an overall vision for how mobile device solutions would support the mission of the organization, creating a high-level strategy for implementing mobile device solutions, developing a mobile device security policy, and specifying business and functional requirements for the solution.
- **Phase 2: Development.** In this phase, personnel specify the technical characteristics of the mobile device solution and related components. These include the authentication methods and the cryptographic mechanisms used to protect communications and stored data. The types of mobile device clients to be used should also be considered, since they can affect the desired policies. Care should be taken to ensure that the mobile device security policy can be employed and enforced by all clients. At the end of this phase, solution components are procured.
- **Phase 3: Implementation.** In this phase, equipment is configured to meet operational and security requirements, including the mobile device security policy documented in the system security plan, installed and tested as a prototype, and then activated on a production network. Implementation includes integration with other security controls and technologies, such as security event logging and authentication servers.
- **Phase 4: Operations and Maintenance.** This phase includes security-related tasks that an organization should perform on an ongoing basis once the mobile device solution is operational, including log review and attack detection.
- **Phase 5: Disposal.** This phase encompasses tasks that occur when a mobile device solution or its components are being retired, including preserving information to meet legal requirements, sanitizing media, and disposing of equipment properly.

This section highlights security considerations of particular interest for mobile device solutions. These considerations are not intended to be comprehensive, nor is there any implication that security elements not listed here are unimportant or unnecessary.

4.1 Initiation

The initiation phase involves many preparatory actions, such as identifying current and future needs, and specifying requirements for performance, functionality, and security. A critical part of the initiation phase is the development of a mobile device security policy for an organization. The section lists elements that a mobile device security policy should contain and, where relevant, describes some of the factors that should be considered when making the decisions behind each element. A mobile device security policy should define which types of mobile devices are permitted to access the organization’s resources, the degree of access that various classes of mobile devices may have (for example, organization-issued devices versus personally-owned devices), and how provisioning should be handled. It should also cover how the organization's centralized mobile device management servers are administered and how policies

in those servers are updated. The mobile device security policy should be documented in the system security plan. To the extent feasible and appropriate, the mobile device security policy should be consistent with and complement security policy for non-mobile systems.

4.1.1 Restrictions on Mobile Devices and Access Levels

An organization's mobile device security policy often limits the types of mobile devices that may be used for enterprise access; this is done for a variety of reasons, including security concerns and technology limitations. For example, an organization might permit only organization-owned mobile devices to be used. Some organizations have tiered levels of access, such as allowing organization-issued mobile devices to access many resources, BYOD mobile devices running the organization's mobile device management client software to access a limited set of resources, and all other BYOD mobile devices to access only a few web-based resources, such as email. This allows an organization to limit the risk it incurs by permitting the most-controlled devices to have the most access and the least-controlled devices to have only minimal access.

Each organization should make its own risk-based decisions about what levels of access should be permitted from which types of mobile devices. Factors that organizations should consider when setting mobile device security policy for this include the following:

- **Sensitivity of work.** Some work involves access to sensitive information or resources, while other work does not. Organizations may have more restrictive requirements for work involving sensitive information, such as permitting only organization-issued devices to be used. Organizations should also be concerned about the legal issues involved in remotely scrubbing sensitive information from BYOD mobile devices.
- **The level of confidence in security policy compliance.** Meeting many of an organization's security requirements can typically be ensured only if the organization controls the configuration of the mobile devices. For devices not running the organization's mobile device management client software, some requirements can possibly be verified by automated security health checks conducted by the mobile device management server when mobile devices attempt to connect, but other requirements cannot be verified.
- **Cost.** Costs associated with mobile devices will vary based on policy decisions. The primary direct cost is issuing mobile devices and client software. There are also indirect costs in maintaining mobile devices and in providing technical support for users.
- **Work location.** Risks will generally be lower for devices used only in the enterprise environment than for devices used in a variety of locations.
- **Technical limitations.** Certain types of mobile devices may be needed, such as for running a particular application. Also, an organization's mobile device management client software may only support certain types of mobile devices.
- **Compliance with mandates and other policies.** Organizations may need to comply with mobile device-related requirements from mandates and other sources, such as a Federal department issuing policy requirements to its member agencies. An example of a possible requirement is restrictions on using mobile devices in foreign countries that have strong known threats against Federal agency systems; in such cases, it may be appropriate to issue "loaner" mobile devices or to prohibit mobile device use altogether.

Organizations may choose to specify additional security requirements that are tied to factors such as the sensitivity of work. Many organizations require more stringent security controls for work situations that

are particularly high-risk, such as permitting the work only from organization-issued and secured mobile devices, and requiring the use of multi-factor authentication for access to the mobile device and to enterprise resources. Another possible security control is to migrate high-risk resources to servers that assume responsibility for protecting them; for example, a mobile device could connect to a server that holds sensitive data that the user needs to access, instead of the sensitive data being stored locally on the mobile device. In high-risk situations, organizations may also choose to reduce risk by prohibiting mobile devices from accessing particular types of information, such as sensitive personally identifiable information (PII).[3]

Every year, there are many changes in mobile device capabilities, the security controls available to organizations, the types of threats made to different types of devices, and so on. Therefore, organizations should periodically reassess their policies for mobile devices and consider changing which types of mobile devices are permitted and what levels of access they may be granted. Organizations should also be aware of the emergence of new types of mobile device solutions and of major changes to existing mobile device management technologies, and ensure that the organization's policies are updated accordingly as needed.

4.1.2 Additional User Requirements

Organizations often have additional security considerations for mobile devices that, while helpful in mitigating threats, cannot necessarily be directly enforced by the organization. Organizations should educate users on the importance of these additional security measures and define users' responsibilities for implementing these measures in policy and mobile device agreements.

One possible security consideration involves wireless personal area networks (WPAN), which are small-scale wireless networks that require no infrastructure to operate. Examples of WPAN technologies are using a wireless keyboard or mouse with a computer, printing wirelessly, synchronizing a mobile device with a computer wirelessly, and using a wireless headset or earpiece with a smart phone. The two most commonly used types of WPAN technologies are Bluetooth and near-field communications. For devices within proximity of significant threats, mobile device users should disable these technologies when not needed to prevent misuse by unauthorized parties. Additional information on these security considerations is available from NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access* [SP800-114], and NIST SP 800-121 Revision 1, *Guide to Bluetooth Security* [SP800-121].

4.2 Development

Once the organization has established a mobile device security policy, identified mobile device needs, and completed other preparatory activities, the next steps are to determine which types of mobile device management technologies should be used and to design a solution to deploy. There are many considerations for designing a solution, most of which are generally applicable to any IT technology; some of these are covered in Section 3 of this document and others in NIST SP 800-53 [SP800-53]. This section focuses on the technical security considerations that are most important for designing mobile device management solutions. Major considerations include the following:

- **Architecture.** Designing the architecture includes the selection of mobile device management server and client software, and the placement of the mobile device management server and other centralized elements.

[3] For more information on protecting PII, see NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* [SP800-122].

- **Authentication.** Authentication involves selecting device and/or user authentication methods, including determining procedures for issuing and resetting authenticators and for provisioning users and/or client devices with authenticators.
- **Cryptography.** Decisions related to cryptography include selecting the algorithms for encryption and integrity protection of mobile device communications, and setting the key strength for algorithms that support multiple key lengths.[4] Federal agencies must use FIPS-approved algorithms contained in validated cryptographic modules when using cryptography to protect information.[5]
- **Configuration requirements.** This involves setting minimum security standards for mobile devices, such as mandatory host hardening measures and patch levels, and specifying additional security controls that must be employed on the mobile device, such as a VPN client.
- **Application vetting and certification requirements.** This sets security, performance, and other requirements that applications must meet and determines how proof of compliance with requirements must be demonstrated.

The security aspects of the mobile device solution design should be documented in the system security plan. The organization should also consider how incidents involving the mobile device solutions should be handled and document those plans as well.[6]

4.3 Implementation

After the mobile device solution has been designed, the next step is to implement and test a prototype of the design, before putting the solution into production. Aspects of the solution that should be evaluated for each type of mobile device include the following:

- **Connectivity.** Users can establish and maintain connections from the mobile device to the organization. Users can connect to all of the organization's resources that they are permitted to and cannot connect to any other organization resources.
- **Protection.** Information stored on the mobile device and communications between the mobile device and the organization are protected in accordance with the established requirements.
- **Authentication.** Authentication is required and cannot be readily compromised or circumvented. All device, user, and domain authentication policies are enforced.
- **Applications.** The applications to be supported by the mobile device solution function properly. All restrictions on installing applications are enforced.
- **Management.** Administrators can configure and manage all components of the solution effectively and securely. The ease of deployment and configuration is particularly important. Another concern is the ability of users to alter device/client software settings, which could weaken mobile device security.

---

4 NIST SP 800-21, Second Edition, *Guideline for Implementing Cryptography in the Federal Government*, presents guidelines for selecting, specifying, employing, and evaluating cryptographic protection mechanisms in Federal information systems. It defines a process for selecting cryptographic products and discusses implementation issues, including solution management, key management, and authentication. [SP800-21]

5 The Cryptographic Module Validation Program (CMVP) at NIST coordinates FIPS 140-2 testing; the CMVP Web site is located at http://csrc.nist.gov/cryptval/. See http://csrc.nist.gov/cryptval/des.htm for information on FIPS-approved symmetric key algorithms, and http://csrc.nist.gov/cryptval/dss.htm for information on digital signature algorithms. See FIPS 140-2, *Security Requirements for Cryptographic Modules*, for more information. [FIPS140-2]

6 For more information on incident handling, see [SP800-61].

- **Logging.** The mobile device solution logs security events in accordance with the organization's policies. See NIST SP 800-92, *Guide to Computer Security Log Management*, for additional information on logging.
- **Performance.** All components of the solution provide adequate performance during normal and peak usage. It is important to also consider the performance of intermediate devices, such as routers and firewalls.
- **Security of the Implementation.** The mobile device implementation itself may contain vulnerabilities and weaknesses that attackers could exploit. Organizations with high security needs may choose to perform extensive vulnerability assessments against the mobile device solution components. At a minimum, all components should be updated with the latest patches and configured following sound security practices. Also, jailbroken and rooted phones should be automatically detected to prohibit their use, for cases in which detection is feasible.
- **Default Settings.** Implementers should carefully review the default values for each mobile device setting and alter the settings as necessary to support security requirements. Implementers should also ensure that the mobile device solution does not unexpectedly "fall back" to insecure default settings for interoperability or other reasons.

Organizations should fully secure each organization-issued mobile device before allowing a user to access it. Any already-deployed mobile device with an unknown security profile (e.g., unmanaged device) should be recovered, restored to a known good state, and fully secured before returning it to its user.

4.4 Operations and Maintenance

Operational processes that are particularly helpful for maintaining mobile device security, and thus should be performed regularly, include the following:

- Checking for upgrades and patches to the mobile device software components, and acquiring, testing, and deploying the updates
- Ensuring that each mobile device infrastructure component (mobile device management servers, authentication servers, etc.) has its clock synced to a common time source so that its timestamps will match those generated by other systems
- Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs
- Detecting and documenting anomalies within the mobile device infrastructure. Such anomalies might indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.
- Providing training and awareness activities for mobile device users on threats and recommended security practices

Organizations should also periodically perform assessments to confirm that the organization's mobile device policies, processes, and procedures are being followed properly. Assessment activities may be passive, such as reviewing logs, or active, such as performing vulnerability scans and penetration testing. More information on technical assessments is available from NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* [SP800-115].

4.5 Disposal

Before a mobile device component permanently leaves an organization (such as when a leased server's lease expires or when an obsolete mobile device is being recycled), the organization should remove any sensitive data from the host. The task of scrubbing all sensitive data from storage devices such as hard drives and memory cards is often surprisingly difficult because of all the places where such data resides and the increasing reliance on flash memory instead of magnetic disks. See NIST SP 800-88, *Guidelines for Media Sanitization* [SP800-88], for additional information and recommendations on removing data from mobile devices. An organization should strongly consider erasing all organization-issued storage devices completely.

Appendix A—Supporting NIST SP 800-53 Security Controls and Publications

The major controls in the NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* control catalog that affect enterprise mobile device security are:

AC-3, Access Enforcement

Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9

AC-4, Information Flow Enforcement

Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18

AC-17, Remote Access

Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121

AC-19, Access Control for Mobile Devices

Related controls: MP-4, MP-5

References: NIST Special Publications 800-114, 800-124

AC-20, Use of External Information Systems

Related controls: AC-3, AC-17, PL-4

References: FIPS Publication 199

CA-7, Continuous Monitoring

Related controls: CA-2, CA-5, CA-6, CM-3, CM-4

References: NIST Special Publications 800-37, 800-53A; US-CERT Technical Cyber Security Alerts; DOD Information Assurance Vulnerability Alerts

CM-6, Configuration Settings

Related controls: CM-2, CM-3, SI-4

References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: nvd.nist.gov; www.nsa.gov)

IA-2, Identification and Authentication (Organizational Users)

Related controls: AC-14, AC-17, AC-18, IA-4, IA-5

References: HSPD 12; OMB Memorandum 04-04; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78

IA-3, Device Identification and Authentication

Related controls: AC-17, AC-18

IA-5, Authenticator Management

Related controls: AC-2, IA-2, PL-4, PS-6

References: OMB Memorandum 04-04; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78

SC-4, Information in Shared Resources

SC-7, Boundary Protection

Related controls: AC-4, IR-4, SC-5

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77

SC-8, Transmission Integrity

Related controls: AC-17, PE-4

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; NSTISSI No. 7003

SC-9, Transmission Confidentiality

Related controls: AC-17, PE-4

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-113; CNSS Policy 15; NSTISSI No. 7003

SC-28, Protection of Information at Rest

References: NIST Special Publications 800-56, 800-57, 800-111

SI-2, Flaw Remediation

Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11

References: NIST Special Publication 800-40

SI-4, Information System Monitoring

Related controls: AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94

SI-7, Software and Information Integrity

Information on these controls and guidelines on possible implementations can be found in the following publications:

- *SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- *SP 800-40 Version 2.0, Creating a Patch and Vulnerability Management Program*
- *SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy*
- *SP 800-46 Rev. 1, Guide to Enterprise Telework and Remote Access Security*
- *SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*
- *SP 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations*
- *SP 800-53A Rev. 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations*

- *SP 800-57, Recommendation for Key Management*
- *SP 800-61 Rev. 1, Computer Security Incident Handling Guide*
- *SP 800-63 Rev. 1, E-Authentication Guideline*
- *SP 800-70 Rev. 2, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*
- *SP 800-73-3, Interfaces for Personal Identity Verification*
- *Draft SP 800-76-2, Biometric Data Specification for Personal Identity Verification*
- *SP 800-77, Guide to IPsec VPNs*
- *SP 800-78-3, Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)*
- *SP 800-81 Rev. 1, Secure Domain Name System (DNS) Deployment Guide*
- *SP 800-83, Guide to Malware Incident Prevention and Handling*
- *SP 800-92, Guide to Computer Security Log Management*
- *SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)*
- *SP 800-111, Guide to Storage Encryption Technologies for End User Devices*
- *SP 800-113, Guide to SSL VPNs*
- *SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access*
- *SP 800-121 Revision 1, Guide to Bluetooth Security*
- *SP 800-128, Guide for Security-Focused Configuration Management of Information Systems*
- *FIPS 140-2, Security Requirements for Cryptographic Modules*
- *FIPS 197, Advanced Encryption Standard*
- *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*
- *FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors*

Appendix B—Acronyms and Abbreviations

Selected acronyms and abbreviations used in this publication are defined below.

BYOD	Bring Your Own Device
CMVP	Cryptographic Module Validation Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GPS	Global Positioning System
IT	Information Technology
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIN	Personal Identification Number
QR	Quick Response
SP	Special Publication
VPN	Virtual Private Networking
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WPAN	Wireless Personal Area Network

Appendix C—Resources

The lists below provide examples of resources that may be helpful in better understanding mobile device security.

[FIPS140-2] FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 2001. http://csrc.nist.gov/publications/PubsFIPS.html#140-2

[FIPS199] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004. http://csrc.nist.gov/publications/PubsFIPS.html#199

[SP800-21] NIST SP 800-21-1, *Guideline for Implementing Cryptography in the Federal Government, Second Edition*, 2005. http://csrc.nist.gov/publications/PubsSPs.html#800-21

[SP800-53] NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, 2009. http://csrc.nist.gov/publications/PubsSPs.html#800-53

[SP800-61] NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*, 2008. http://csrc.nist.gov/publications/PubsSPs.html#800-61

[SP800-88] NIST SP 800-88, *Guidelines for Media Sanitization*, 2006. http://csrc.nist.gov/publications/PubsSPs.html#800-88

[SP800-111] NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, 2007. http://csrc.nist.gov/publications/PubsSPs.html#800-111

[SP800-114] NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, 2007. http://csrc.nist.gov/publications/PubsSPs.html#800-114

[SP800-115] NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, 2008. http://csrc.nist.gov/publications/PubsSPs.html#800-115

[SP800-121] NIST SP 800-121 Revision 1, *Guide to Bluetooth Security*, 2012. http://csrc.nist.gov/publications/PubsSPs.html#800-121

[SP800-122] NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, 2010. http://csrc.nist.gov/publications/PubsSPs.html#800-122

Mobile Device Security-Related Checklist Sites

Site	URL
DISA Security Technical Implementation Guides (STIGs)	http://iase.disa.mil/stigs/index.html
DISA Wireless (Smartphone/Tablet) STIGs	http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html
NIST National Checklist Program Repository	http://web.nvd.nist.gov/view/ncp/repository